PROPONER UN PLAN DE GESTIÓN DE RIESGO OPERATIVO EN EL ÁREA DE DESARROLLO DE LA EMPRESA VYG TECNOLOGÍA Y SOLUCIONES

GINETH ÁVILA VELANDIA
LUIS CARLOS BOBADILLA MORENO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2015

PROPONER UN PLAN DE GESTIÓN DE RIESGO OPERATIVO EN EL ÁREA DE DESARROLLO DE LA EMPRESA VYG TECNOLOGÍA Y SOLUCIONES

GINETH ÁVILA VELANDIA
LUIS CARLOS BOBADILLA MORENO

PROYECTO DE INVESTIGACIÓN

LORENA OCAMPO CORREA
INGENIERO DE SISTEMAS ESPECIALISTA EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2015

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 21 de Agosto de 2015

CONTENIDO

LISTA DE CUADROS

pág.

LISTA DE GRÁFICAS

pág.

LISTA DE ANEXOS

pág.

0. INTRODUCCIÓN

Todos los procesos de las organizaciones están expuestos a riesgos, por lo tanto, para que se tenga éxito en la gestión de riesgos todos los integrantes de la empresa deben estar en continua participación, desde la alta gerencia, hasta donde se ejecuta cada proceso. Las personas responsables directas de cada actividad o proceso, deben tener identificados los riesgos, que involucran a las actividades que pertenecen y gestionarlos.

Diferentes investigaciones sobre desastres financieros en la historia, han clasificado el riesgo operacional como el principal responsable. Por lo tanto se debe fortalecer la cultura de gestión de riesgo operacional para estar mejor preparados ante eventualidades y que estas se conviertan en oportunidades, para que la actividad de la empresa se vea alterada de la menor manera posible.

El riesgo operacional de un área puede afectar a otras áreas de la empresa, de ahí la importancia de generar una cultura de gestión de riesgo operacional, que impida que el riesgo se propague y se manifiesten a través de los procesos de la empresa.

El presente proyecto de investigación fue realizado con el objetivo de justificar la necesidad de implementar un plan de gestión de riesgos para la empresa VYG Tecnología y Soluciones que contenga los controles necesarios para mitigar los riesgos o disminuirlos a un nivel aceptable.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 FORMULACIÓN DEL PROBLEMA

¿De qué forma la empresa V&G Tecnología y Soluciones podrá manejar los riesgos operacionales en el área de desarrollo para no afectar el desempeño del área y la eficacia del servicio de la empresa?

1.2 JUSTIFICACIÓN

El propósito de la siguiente propuesta es realizar un análisis de plan de gestión de riesgos operacionales que le va a permitir a la empresa estar preparada contra amenazas que se presentan en la actualidad, como es la falta de conocimiento del personal de seguridad de la información en lo que se refiere a la ejecución de sus actividades como por ejemplo: realizar copias de respaldo de la información. En muchas ocasiones se pierde información en los equipos de los analistas técnicos de desarrollo por problemas en circuito eléctrico que conllevan a que se apaguen los servidores y por lo tanto se detenga el trabajo, ocasionando también pérdida de archivos que no se hayan guardado, afectando el objetivo de la empresa.

Es necesaria la implementación de un plan de gestión de riesgos operacionales en el área de desarrollo de software para detectar qué vulnerabilidades tiene la empresa VYG Tecnología y Soluciones. Identificar las amenazas a que estaría expuesta la empresa que pueden atacar en cualquier momento el normal funcionamiento de la misma; establecer el valor de los activos para conocer qué impacto pueden tener estas amenazas y a partir de esto, establecer controles que permitan mitigar o reducir el riesgo a un nivel aceptable que pueda asumir la organización.

En caso de que ocurra un desastre como un terremoto o ingresaran a la organización personas ajenas a la empresa y se perdiera toda la información, la empresa puede incurrir en pérdidas legales y financieras. Adicionalmente se pueden perder avances en desarrollos de software que corresponden a días de trabajo que se tendrían que pagar nuevamente a los analistas técnicos para que vuelvan a generar la información.

Con el plan de gestión de riesgos operacionales VYG Tecnología y Soluciones podrá contar con procedimientos y controles que le van a permitir salvaguardar a la empresa de los diferentes riesgos que se pueden presentar, evitando pérdidas financieras, institucionales y/o legales lo que ocasiona un impacto negativo.

1.3 OBJETIVOS

1.3.1 Objetivo general. Realizar una propuesta de gestión de riesgo operativo en el área de desarrollo de VYG tecnología y soluciones, con el fin de proporcionarle una mayor seguridad a la información.

1.3.2 Objetivos específicos. Para conseguir exitosamente el objetivo general de este proyecto, se deben cumplir antes los siguientes objetivos:

- Identificar los activos que hacen parte de la empresa.
- Identificar las posibles amenazas que se pueden presentar en la ejecución de las funciones en el área de desarrollo.
- Identificar las diferentes vulnerabilidades que se presentan en el área de desarrollo.
- Realizar propuesta de plan de gestión de riesgo operativo para el área de desarrollo.

2. MARCO TEÓRICO

2.1 ANTECEDENTES

En el transcurso de la historia las personas han convivido con diferentes tipos de riesgos como por ejemplo, los ocasionados por la naturaleza: terremotos, incendios forestales, inundaciones, actos malintencionados generados por otros seres humanos y otros riesgos. La supervivencia a estos riesgos se realizaba de forma natural.

En los últimos años tras la ejecución de las nuevas tecnologías en el sector bancario, administrativo; se ha visto la necesidad de implementar métodos y procedimientos que ayuden a proteger de amenazas los activos de la organización y que pueden afectar la disponibilidad, integridad y confidencialidad de la información.

En todo tipo de actividad económica estará siempre presente el riesgo operativo. Las empresas deben realizar actividades como lo es la gestión, identificación, evaluación y mitigación de los riesgos. Las organizaciones que saben advertir y adelantarse a los posibles riesgos que se pueden presentar y que tienen técnicas o procedimientos de actuación para riesgos operacionales pueden evitar enormes pérdidas.

La severidad de los riesgos operacionales es muy extensa, pudiendo conllevar desde una pequeña pérdida para la compañía hasta su desaparición, como ha ocurrido de manera notoria en empresas financieras, de servicios o del sector Bancario. La necesidad de que el directivo se adelante al hecho se puede observar en muchas circunstancias de la vida empresarial.

En el contexto empresarial el riesgo puede definirse como: "los factores, acontecimientos, tanto internos como externos, a que está expuesta la empresa, y que ponen en peligro la consecución de los objetivos".

Es el caso de los bancos Barings del Reino Unido y el japonés Daiwa ocurridos en 1995, así como la quiebra de las empresas estadounidenses Enron en 2001 y Worldcom en 2002 (Deloitte, 2004). Dichos eventos, además, han impactado no solo la forma de administrar los riesgos de las empresas en diferentes sectores

económicos, sino también la estructura de los sistemas de control y las regulaciones existentes del sector financiero internacional[1].

En este orden de ideas, una buena gestión de riesgos requiere de una visión estratégica en la que participen activamente los miembros que se encuentran desde la alta gerencia de la organización hasta los funcionarios que lideran la ejecución de los procesos.

2.2 MARCO INSTITUCIONAL

V&G Tecnología y Soluciones es una organización con ánimo de lucro dedicada a la implementación de soluciones de software para el sector financiero cuya sede principal se encuentra ubicada en Bogotá en la calle 39 28-09 oficina 502 Soledad.

La organización actualmente está conformada por 140 trabajadores de los cuales 80 son internos, y los 60 restantes son externos.

Debido a las diferentes amenazas y vulnerabilidades a que se encuentran expuestas hoy en día las organizaciones, y la importancia de proteger correctamente los recursos de la organización, V&G Tecnología y Soluciones tiene la necesidad de adquirir un plan de gestión de riesgos operacionales que le proporcionará políticas y procedimientos para la gestión del riesgo en el área de desarrollo basado en la norma técnica colombiana NTC 5254, ISO/IEC 27001 y ISO/IEC 27005.

[1] AD-MINISTER. Administración del riesgo operacional en Colombia. Disponible desde internet desde. http://publicaciones.eafit.edu.co/index.php/administer/article/viewFile/553/499] pág.2, (consultado el 29 de agostos 2014

3. DISEÑO METODOLÓGICO

Este proyecto está orientado hacia una metodología de investigación de tipo descriptiva y explicativa por lo tanto el desarrollo metodológico se ejecutara de acuerdo a los parámetros y directrices planteados en la norma NTC 5254, ISO/IEC 27001 y ISO/IEC 27005.

3.1 POBLACIÓN Y MUESTRA

3.1.1 Población. La población son todos los funcionarios de la organización.

3.1.2 Muestra. La muestra que se tomó como estudio fue el área de desarrollo de la organización.

3.2 UNIDAD DE ANÁLISIS

Como unidad de análisis en este proyecto se tendrá en cuenta cada uno de los riesgos de seguridad de la información, detectados en el área de desarrollo de la organización.

3.3 FASES SEGÚN EL TEMA

3.3.1 Identificación y valoración de los activos. Se realiza la valoración de los activos con respecto a los tres elementos de la seguridad de la información, que son confidencialidad, integridad y disponibilidad. Para ello se indago a cada uno de los responsables.

3.3.2 Identificación de las vulnerabilidades, amenazas y cálculo de los riesgos. Después de haber identificado y valorado los activos se inicia el proceso de identificar las vulnerabilidades y amenazas, clasificándolas por cada tipo de activo según la norma ISO/IEC 27005 para el cálculo de los riesgos.

3.3.3 Planteamiento de acciones para plan de gestión de riesgos. Terminadas las dos fases anteriores se procede a la identificación de los controles para los riesgos y las medidas de defensa, teniendo en cuenta el impacto y el nivel de aceptación de los riesgos en la organización**.**

4. DESARROLLO Y EJECUCIÓN DEL PROYECTO

4.1 ANÁLISIS DE RIESGO

4.1.1 Identificación y valoración de los activos para el área de desarrollo. De acuerdo con el diseño metodológico, en la primera fase se realiza la identificación de los activos para el área de desarrollo, por medio de encuestas con el ingeniero de infraestructura y responsable del área, las cuales se anexan en el presente trabajo.

Se efectuó la clasificación de los activos de acuerdo a la norma ISO/IEC 27005 en su anexo B, como se visualiza en el cuadro 1.

Cuadro 1. Tipos de activos.

Id	Tipos de activo	Activos	Descripción del activo	Responsable
1	Hardware	Computadores de escritorio, Servidor, Disco Duro extraíble.	Equipos donde se guarda la información importante de la empresa como son los desarrollos de software para las diferentes empresas.	Funcionario asignado y líder de infraestructura
2	Software	Microsoft office y las aplicaciones del negocio.	Programas que permiten el funcionamiento del hardware.	Líder de infraestructura
3	Personal	Usuarios finales, alta gerencia, líder de proyectos y desarrolladores.	El grupo de personas que están involucradas en la organización con el sistema de información del área de desarrollo.	Gerente
4	Lugar	Edificio, oficinas y centro de cómputo.	Sitios y medios físicos que son muy importantes para el correcto funcionamiento.	Líder de infraestructura
5	Organización	Proveedores, fabricantes, servicios, proyectos, estructura de la organización.	Entidades que suministran a la organización un servicio o los recursos.	Gerente

Fuente: Elaboración autores.

Se realizó la valoración de cada activo de acuerdo a los principios de seguridad de la información que es: la confidencialidad, la integridad y disponibilidad, como se muestra en el cuadro 2.

Cuadro 2. Valoración de los activos según la confidencialidad, integridad y disponibilidad de la información.

Nivel	Valoración	Descripción
1	Insignificante	La pérdida de confidencialidad, Integridad o Disponibilidad generará perdidas insignificantes en el incumplimiento de la legislación y/o reglamentación, deterioro en el desempeño del negocio, pérdidas financieras o pérdida del buen nombre de la organización.
2	Bajo	La pérdida de confidencialidad, Integridad o Disponibilidad generará perdidas bajas en el incumplimiento de la legislación y/o reglamentación, deterioro en el desempeño del negocio, pérdidas financieras o pérdida del buen nombre de la organización.
3	Moderado	La pérdida de confidencialidad, Integridad o Disponibilidad generará perdidas moderadas en el incumplimiento de la legislación y/o reglamentación, deterioro en el desempeño del negocio, pérdidas financieras o pérdida del buen nombre de la organización.
4	Alto	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas altas en el incumplimiento de la legislación y/o reglamentación, deterioro en el desempeño del negocio, pérdidas financieras o pérdida del buen nombre de la organización.
5	Extremo	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas totales en el incumplimiento de la legislación y/o reglamentación, deterioro en el desempeño del negocio, pérdidas financieras o pérdida del buen nombre de la organización.

Fuente: Elaboración autores.

Después de haber generado la clasificación y valoración de los de activos de acuerdo con la norma ISO/IEC 27005 en su anexo B, a continuación se muestra la información de los activos que hacen parte del área de desarrollo, como se observa en el cuadro 3.

Cuadro 3. Activos del área de desarrollo.

Id	Activos	Cantidad	Descripción
1	Computadores de escritorio	48	Máquinas tipo desktop con las siguientes características: • HP COMPAQ 6305 pro desktop • Memoria de 2 GB RAM • Disco duro de 300 GB • Procesador 2.8 GHZ • Sistema operativo Windows 7 pro • Monitor 17 pulgadas
2	Portátil	2	Maquinas tipos portátil con las siguientes características: • Thinkpad T420 • Memoria de 4 GB RAM • Procesador Core I5 2,8 GHZ • Sistema Operativo Windows 8.
3	Disco duro extraíble	1	Discos duros externos marca Toshiba de 3 TB cada uno con velocidad de transferencia de 5 GBPS y USB 3.0, se utilizan para respaldo de información.
4	Impresoras	1	Impresora Hp Multifuncional 1515 Deskjet con las siguientes características: • Velocidad de impresión en negro ISO: Hasta 7 ppm [1] Borrador: Hasta 20 ppm. • Velocidad de impresión a color: ISO: Hasta 4 ppm [1]. • Número de cartuchos de impresión: 2 (1 negro, 1 tricolor) • Ciclo de trabajo (mensual, A4): Hasta 1000 páginas.

Cuadro 3. (Continuación).

Id	Activos	Cantidad	Descripción
5	Servidores	2	• Los dos servidores tienen las mismas características: • • Marca HP Proliant ML 350 G6. • Memoria de 16 GB RAM. • Procesadores Quadcore de 2.6 GHZ. • Discos duros de 200 GB cada uno. • Sistema operativo Windows 2008 Enterprise. • • Este servidor esta designado para la Vitalización utilizando VMWare, servidor de archivos y Firewall.
6	Funcionarios	50	Alta gerencia, técnicos, ingenieros, administradores de empresas.
7	Ventiladores	4	Ventiladores con las siguientes características: • Marca: SAMURAI. • Potencia Del Motor: 80W. • Servicios: Pared. • Tamaño De Las Aspas: 18 Pulgadas. • Material: Plástico. • Garantía: 24 Meses. • Dimensiones: 60x30x70. • Color: Blanco.
8	Sillas	48	Sillas tipo Oficina. Medidas: • Diámetro base 51,8 cm. • Alto espaldar 38 cm. • Ancho 50 cm. • Altura hasta asiento 30 cm. • Alto 52 cm. • Profundidad asiento 38 cm. Características: • Silla con palanca para graduar la altura de la silla.

Cuadro 3. (Continuación).

Id	Activos	Cantidad	Descripción
9	Escritorio computador	48	Escritorios de 1,20 de largo y 80 cm de ancho. Color blanco con gris, cada uno cuenta con cajón para guardar implementos de trabajo.
10	Video Beam	1	Video Beam marca Epson PowerLite. Cinema: 730HD / 3.000. Lumens / WXGA 1280 x800 (720p) /. Contraste: 12.000:1 / Vida útil de la lámpara: 4.000 Horas Normal. 5.000 ECO / Tamaño: 33". Entrada: 480i / 576i / 480p / 576p / 720p / 1080i / 1080p HDMI: TMDS.

Fuente: Elaboración autores.

A continuación se muestra en el cuadro 4 la valoración de los activos de la organización tomando como referencia la norma NTC 5254 en su anexo E.

Cuadro 4. Métricas para la valoración del impacto de los activos.

No	Tipos de activo	Activos	Integridad	Disponibilidad	Confidencialidad	Impacto
1	Hardware	Computadores de escritorio, Servidor, Disco Duro extraíble.	4	4	4	4
2	Software	Sistemas Operativos y las aplicaciones del negocio.	4	4	4	4
3	Personal	Usuarios finales, alta gerencia, líder de proyectos y desarrolladores.	4	4	4	4
4	Lugar	Casa, oficinas y centro de cómputo.	4	4	4	4
5	Organización	servicio , proveedores, proyectos.	4	4	4	4

Fuente: Elaboración autores.

Se realizó la valoración del impacto de acuerdo a los 3 principios de la seguridad de la información que son la confidencialidad, integridad y disponibilidad.

Para la valoración dada en el cuadro 4, se estableció el valor cuatro (4) impacto mayor, que hace referencia a lesiones grandes, pérdida de la capacidad de producción y pérdida financiera importante.

4.1.2 Identificación de las amenazas. Se Inicia el proceso de evaluación de las amenazas con respecto a la norma ISO/IEC 27005 en su anexo C. Estas pueden explotar una o varias vulnerabilidades; al no tener un control sobre las amenazas estas pueden presentar incidentes que afectan a la organización.

Las amenazas pueden ser de orígenes accidentales(A), deliberados (D) y/o ambientales (E) como se enseñan en el cuadro 5.

Cuadro 5. Origen de las amenazas.

Id	Origen	Descripción
A	Accidentales	Se utiliza para las acciones humanas que pueden dañar accidentalmente los activos de información.
D	Deliberadas	Tienen como objetivo los activos de la información.
E	Ambientales	Todos los incidentes que no se basan en las acciones humanas.

Fuente: Elaboración autores.

Después de haber identificado los criterios del origen de las amenazas, teniendo como referencia la norma ISO/IEC 27005 de su Anexo C, se inicia el proceso de identificar las amenazas del área de desarrollo, obteniendo como resultado la información del cuadro 6.

Cuadro 6. Amenazas detectadas en el área de desarrollo.

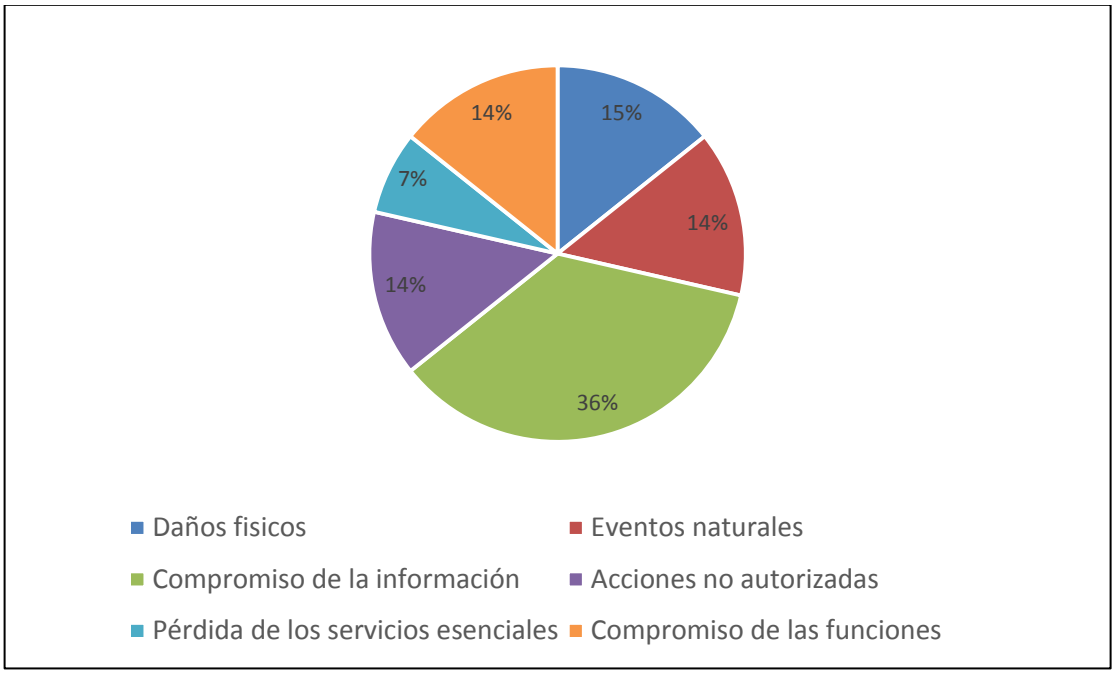
No	Amenazas	Tipo de amenaza	Origen	Ejemplos
1	Fuego.	Daños físicos	A,D	Se evidencia que los funcionarios ingresan mecheras para encender cigarrillos. Se recalientan los cables de los computadores debido a la carga de energía.
2	Daño por ingreso de alimentos.		A,D,E	Los funcionarios ingresan bebidas al puesto de trabajo.
3	Daños por polvo.		A,D,E	Se evidencia que no se realiza mantenimiento a los equipos de cómputo.
4	Fenómeno Sísmico.	Eventos naturales	E	Posibilidad de que ocurra un terremoto.
5	Espionaje remoto.	Compromiso de la información	D	Persona no autorizada a la organización.
6	Hurtos de medios, documentos o equipos.		D	Al no existir inventario de los activos se puede presentar el caso de hurto. Podrían ingresar personas con el fin de hurtar los equipos o elementos de valor de la empresa.

Cuadro 6. (Continuación).

No	Amenazas	Tipo de amenaza	Origen	Ejemplos
7	Divulgación	Compromiso de la información.	A,D	Funcionarios de la empresa podrían divulgar información sensible de la empresa.
8	Manipulación de Software		A,D	Al no existir perfiles de acceso a los equipos de la empresa, cualquier funcionario puede acceder y realizar cambios.
9	Perdida de información		A,D	Al no existir un procedimiento para sacar copias de respaldo
10	Uso no autorizado del equipo	Acciones no autorizadas.	A,D	Funcionarios de la empresa podrían divulgar información sensible de la empresa.
11	Ingreso a la empresa sin autorización		A,D	Al no existir perfiles de acceso a los equipos de la empresa, cualquier funcionario puede acceder y realizar cambios.
12	Pérdida de suministro de energía	Pérdida de los servicios esenciales	A,D,E	Cuando se va el servicio de energía. Robo de cables de la energía.
13	Error en el uso	Compromiso de las funciones	A	Uso inadecuado de software.
14	Abuso de derechos		A,D	Inicio de sesión al sistema sin previa autorización.

Fuente: Elaboración autores.

Gráfica 1. Amenazas detectadas en el área de desarrollo.



Fuente: Elaboración autores.

Como se observa en la gráfica 1 el tipo de amenaza más vulnerable es el compromiso de la información con un 36% del total de las amenazas detectadas en el área de desarrollo. Lo anterior quiere decir que la empresa estaría más susceptible a que personas no autorizadas ingresen al sistema; adicional que al no existir perfiles de acceso a los equipos de la empresa cualquier funcionario puede acceder y realizar cambios afectando la integridad de la información. También pueden presentarse casos de hurto ya que la empresa no cuenta con un inventario de activos.

4.1.3 Identificación de vulnerabilidades. Terminado el proceso de identificar las amenazas y los activos evidenciamos con ayuda de la norma ISO/IEC 27005 en su anexo D, que las amenazas identificadas explotan 21 vulnerabilidades.

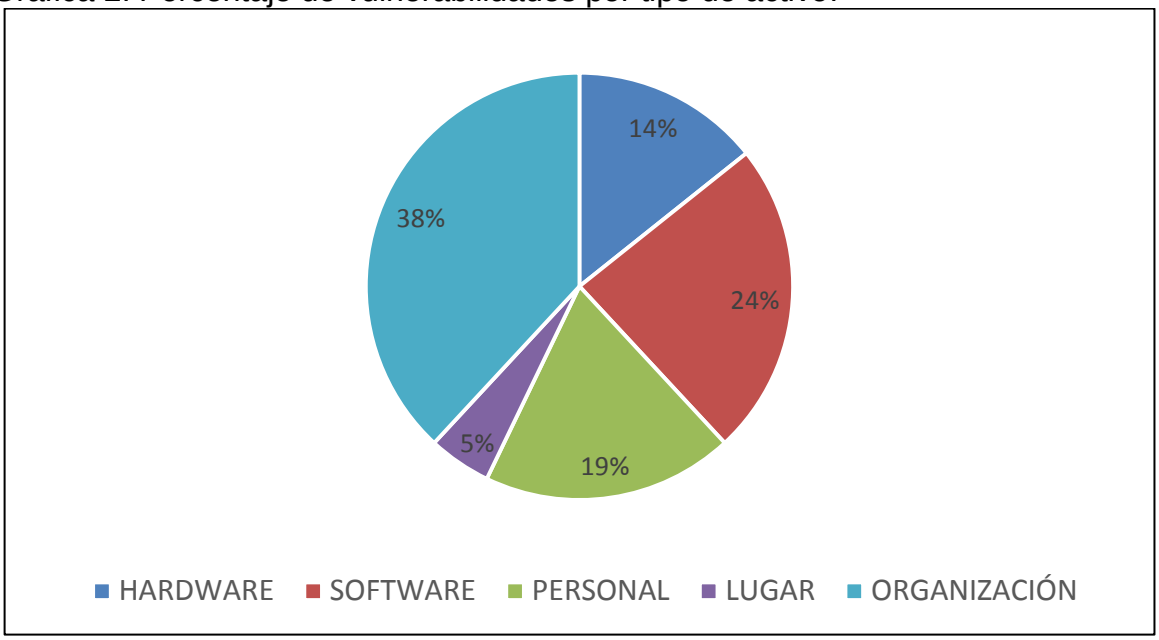
De acuerdo a lo anterior se relacionan en el cuadro 7 la lista de vulnerabilidades con relación a los activos de la empresa.

Cuadro 7. Vulnerabilidades detectadas en el área de desarrollo.

No	Descripción de la vulnerabilidad	Tipo de activo
1	Susceptibilidad a la humedad, el polvo y la suciedad.	HARDWARE
2	Susceptibilidad a las variaciones de tensión.	
3	Almacenamiento sin protección.	
4	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.	SOFTWARE
5	Falta de mecanismos de identificación y Autentificación.	
6	Gestión deficiente de las contraseñas.	
7	Descarga y uso no controlados de software.	
8	Falta de copias de respaldo.	
9	Entrenamiento insuficiente en seguridad.	PERSONAL
10	Uso incorrecto de software y hardware.	
11	Falta de conciencia acerca de la seguridad.	
12	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.	
13	Red energética inestable.	LUGAR
14	Falta de procedimiento de monitoreo de los recursos de procesamiento información.	ORGANIZACIÓN
15	Falta de procedimientos de identificación y evaluación de riesgos.	
16	Falta de procedimiento formal para la autorización de la información disponible al público.	
17	Falta de planes de continuidad.	
18	Falta de políticas sobre el uso del correo electrónico.	
19	Falta de procedimientos para el manejo de información clasificada.	
20	Falta de responsabilidades en la seguridad de la información en la descripción de los cargos	
21	Falta de política formal sobre la utilización de computadores portátiles	

Fuente: Elaboración autores.

Gráfica 2. Porcentaje de vulnerabilidades por tipo de activo.



Fuente: Elaboración autores.

Se observa en la gráfica 2 que el mayor porcentaje de vulnerabilidades se identificaron en el tipo de activo organización con un 38% del total de las vulnerabilidades. Las vulnerabilidades con mayor tendencia a ser explotadas por amenazas en el área de desarrollo son las siguientes:

- Faltan procedimientos de monitoreo de los recursos de procesamiento de información.
- Faltan procedimientos de identificación y evaluación de riesgos.
- Faltan planes de continuidad.
- Faltan políticas sobre el uso del correo electrónico.
- Faltan responsabilidades en la seguridad de la información en la descripción de los cargos.
- Falta de procedimiento formal para la autorización de la información disponible al público.

A continuación se describen en el cuadro 8 los niveles de probabilidad de ocurrencia, para los cuales se tomó como referencia la norma NTC 5254 en su anexo E.

Cuadro 8. Métricas para la probabilidad de ocurrencia.

Nivel	Probabilidad	Descripción
1	Casi cierto	Puede ocurrir varias veces durante el año.
2	Probable	Existe la posibilidad de que ocurra varias veces, ha ocurrido una vez en último año.
3	Posible	Posiblemente ocurra en algún momento, ha ocurrido una vez en 3 años, es posible que ocurra durante el año.
4	Improbable	Puede suceder en pocas circunstancias, ha pasado una vez en los últimos 5 años, difícil que ocurra durante el año.
5	Raro	Posiblemente se presente en circunstancias excepcionales, ha ocurrido una vez hace 10 años, poco probable que ocurra durante el año.

Fuente: Elaboración autores.

4.2 EVALUACIÓN DEL RIESGO

Al obtener las amenazas, vulnerabilidades y los diferentes valores se obtuvo como resultado el análisis de riesgos, de acuerdo a esto se obtiene el riesgo inherente con la siguiente ecuación:

Riesgo inherente= impacto * probabilidad de ocurrencia

A continuación en el cuadro 9 se muestra el formato que se utilizó para el cálculo del riesgo:

Cuadro 9. Formato para cálculo de riesgo.

No	Tipo de activo	Activos	Propietario	Impacto	Vulnerabilidad	Amenaza	Probabilidad de ocurrencia	Riesgo (inherente)
1	Hardware	Computadores de escritorio, Servidor, Disco duro extraíble.	Jefe de infraestructura	4	Susceptibilidad a la humedad, el polvo y la suciedad.	Daños por polvo.	2	8
					Susceptibilidad a las variaciones de tensión.	Pérdida de suministro de energía.	3	12
					Almacenamiento sin protección.	Hurtos de medios, documentos o equipos.	3	12
2	software	Sistemas Operativos y las aplicaciones del negocio.		4	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.	Uso no autorizado del equipo.	5	20
					Falta de mecanismos de identificación y Autentificación.		3	12
					Gestión deficiente de las contraseñas.		5	20
					Descarga y uso no controlados de software.	Manipulación con Software.	3	12
					Falta de copias de respaldo.	Pérdida de Información.	4	16

Cuadro 9. (Continuación).

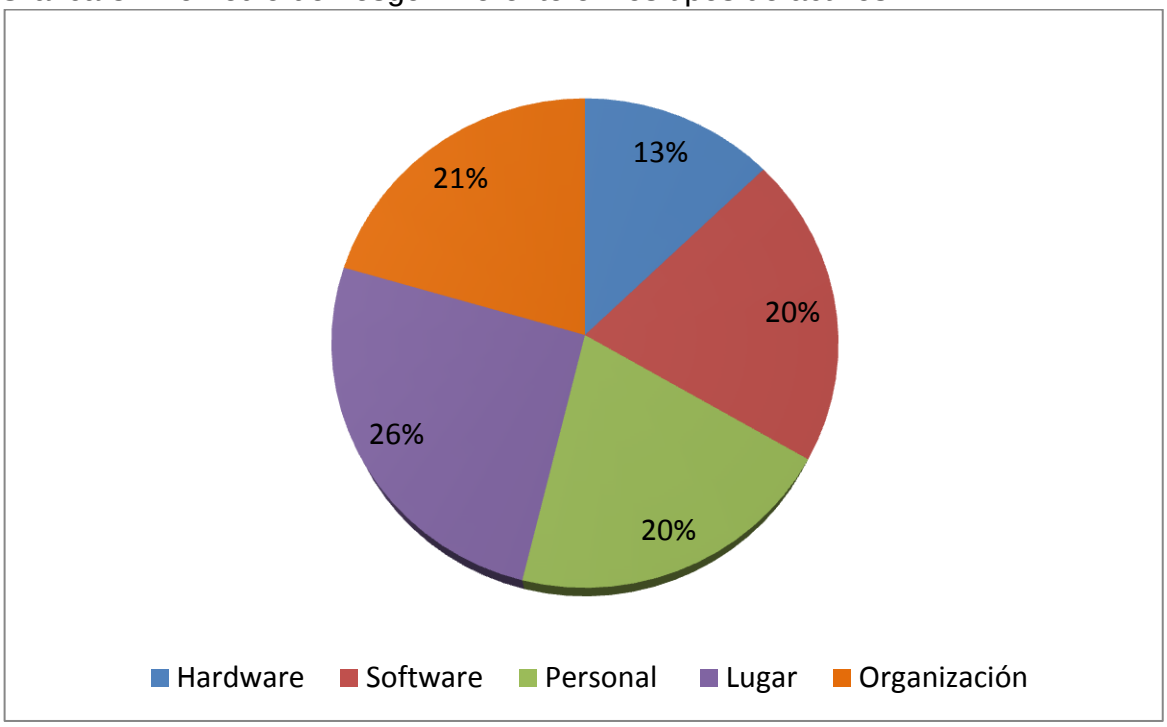
No	Tipo de activo	Activos	Propietario	Impacto	Vulnerabilidad	Amenaza	Probabilidad de ocurrencia	Riesgo (inherente)
3	Personal	Usuarios finales, alta gerencia, líder de proyectos y desarrolladores.	Área de Recursos Humanos	4	Entrenamiento insuficiente en seguridad.	Abuso de derechos	4	16
					Uso incorrecto de software y hardware.		3	12
					Falta de conciencia acerca de la seguridad.		4	16
					Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.		5	20
4	Lugar	Casa, oficinas y centro de cómputo.	Jefe de infra-estructura	4	Red energética inestable.	Pérdida del suministro de energía	5	20
5	Organización	Servicio, proveedores, proyectos.	Gerente	4	Falta de procedimiento de monitoreo de los recursos de procesamiento información.	Abuso de los derechos	4	16
					Falta de procedimientos de identificación y evaluación de riesgos.	Abuso de los derechos	4	16
					Falta de procedimiento formal para la autorización de la información disponible al público.	Divulgación	3	12

Cuadro 9. (Continuación).

No	Tipo de activo	Activos	Propietario	Impacto	Vulnerabilidad	Amenaza	Probabilidad de ocurrencia	Riesgo (inherente)
5	Organización	Servicio , proveedores, proyectos	Gerente	4	Falta de planes de continuidad.	Falla del equipo.	5	20
					Falta de políticas sobre el uso del correo electrónico.	Abuso de los derechos.	5	20
					Falta de procedimientos para el manejo de información clasificada.	Divulgación.	5	20
					Falta de responsabilidades en la seguridad de la información en la descripción de los cargos.	Abuso de los derechos.	4	16
					Falta de política formal sobre la utilización de computadores.	Hurto de equipo.	2	8

Fuente: Elaboración autores.

Gráfica 3. Promedio de riesgo inherente en los tipos de activos.



Fuente: Elaboración autores.

Se observa en la grafica 3 que el tipo de activo con el promedio mas alto de riesgo es lugar (26%), la empresa se ve afectada por la perdida del suministro de energía por contar con una red de energía inestable. Debido a estos resultado se evidencia que la empresa no esta preparada para controlar la perdida de energía en un lapso de tiempo minimo como por ejemplo treinta(30) minutos.

4.3 NIVEL DE ACEPTACIÓN DE RIESGO.

Para el cálculo de nivel de aceptación de riesgo se toma como referencia la norma ISO/IEC 27005 en su anexo E. En conjunto con la gerencia y los encargados de los procesos del área de desarrollo, de acuerdo a las consecuencias evaluadas y la probabilidad se establecen los siguientes rangos para los criterios de evaluación del riesgo se describen en el cuadro 10:

Cuadro 10. Niveles de aceptación del Riesgo.

Escala de probabilidad	Impacto				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Improbable (1)	1	2	3	4	5
Improbable (2)	2	4	6	8	10
Posible (3)	3	6	9	12	15
Probable (4)	4	8	12	16	20
Frecuente (5)	5	10	15	20	25

Fuente: Elaboración autores.

La Gerencia de la organización consideró evaluar los riesgos que estén dentro del rango aceptable (valor de 1-4), moderado (valor de 5-14) e inaceptable (valor de 15 - 25), en razón a que la empresa quiere mejorar de manera significativa la seguridad. Actualmente tiene un bajo nivel de seguridad por lo que el valor de la inversión que desea realizar a corto plazo es medio.

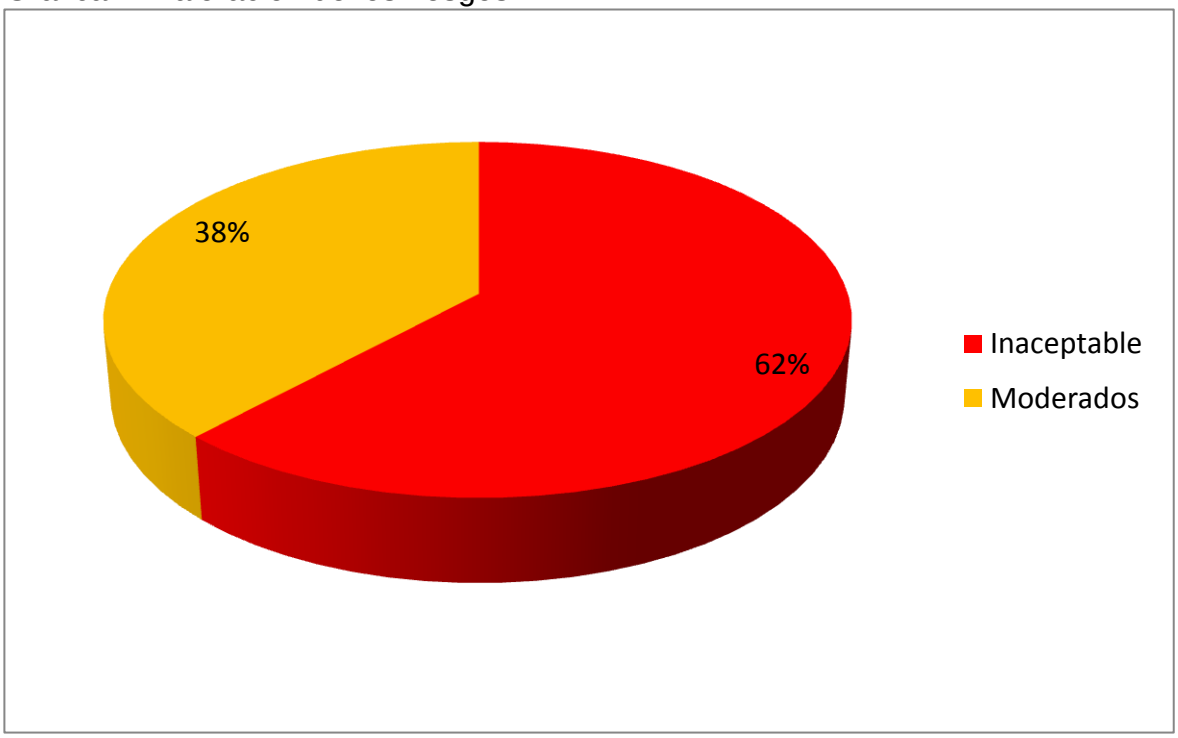
Posteriormente, como resultado se muestra los criterios de evaluación del riesgo en el cuadro 11:

Cuadro 11. Nivel de aceptación y valor del Riesgo.

Nivel de aceptación	Valor
Aceptable	1-4
Moderado	5-14
Inaceptable	15-25

Fuente: Elaboración autores.

Gráfica 4. Valoración de los riesgos.



Fuente: Elaboración autores.

Teniendo en cuenta los niveles de aceptación del riesgo se observa en la gráfica 4 que un 62% de los riesgos se encuentran en un nivel inaceptable de aceptación de riesgo, razón importante por la cual se debe realizar un plan de gestión de riesgos.

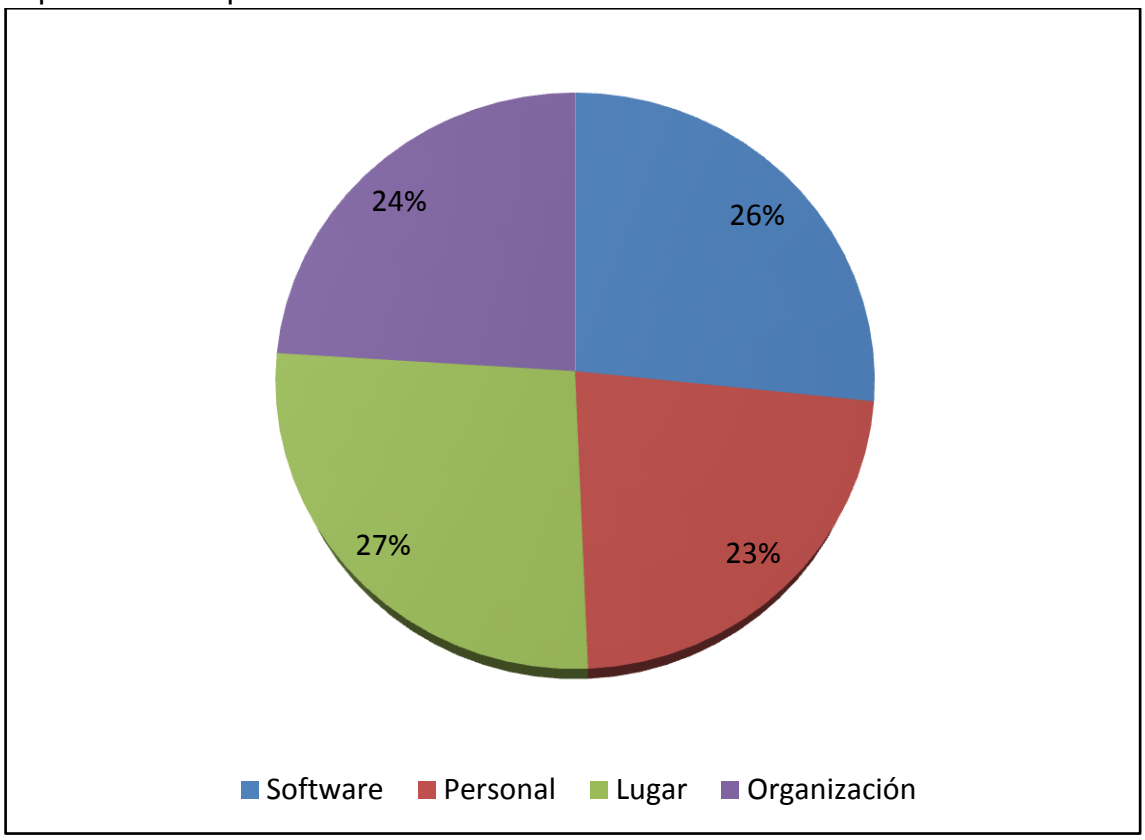
De acuerdo con lo anterior, los riesgos que se encuentran en un nivel de aceptación “Inaceptable” es decir que están dentro del rango de valor de aceptación entre 15–25, un total de 13; se publican en el anexo A (Matriz de resultados) y se exponen en el cuadro 12:

Cuadro 12. Riesgos en nivel inaceptable.

Id	Tipo activo	Vulnerabilidad	Amenaza	Riesgos (inherente)	Nivel de aceptación
1	Software	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.	Uso no autorizado del equipo.	20	Inaceptable
2		Gestión deficiente de las contraseñas.		20	Inaceptable
3		Falta de copias de respaldo.	Pérdida de Información.	16	Inaceptable
4	Personal	Entrenamiento insuficiente en seguridad.	Abuso de derechos.	16	Inaceptable
5		Falta de conciencia acerca de la seguridad.		16	Inaceptable
6		Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.		20	Inaceptable
7	Lugar	Red energética inestable.	Pérdida del suministro de energía.	20	Inaceptable
8	Organización	Falta de procedimiento de monitoreo de los recursos de procesamiento de la información.	Abuso de los derechos.	16	Inaceptable
9		Falta de procedimientos de identificación y evaluación de riesgos.		16	Inaceptable
10		Falta de planes de continuidad.	Falla del equipo	20	Inaceptable
11		Falta de políticas sobre el uso del correo Electrónico.	Abuso de los derechos	20	Inaceptable
12		Falta de procedimientos para el manejo de información clasificada.	Divulgación	20	Inaceptable
13		Falta de responsabilidades en la seguridad de la información en la descripción de los cargos.	Abuso de los derechos	16	Inaceptable

Fuente: Elaboración autores.

Gráfica 5. Porcentaje de riesgo inherente en los tipos de activos con un nivel de aceptación inaceptable.



Fuente: Elaboración autores.

Se aprecia en la gráfica 5 que el promedio mas alto de riesgo inherente con un nivel inaceptable de aceptación lo esta ocupando el tipo de activo “lugar” , como se ha venido evidenciando este tipo de activo se afecta por la perdida de suministro de energía y la red inestable, afectando los objetivos de la organización. Esto se debe que la empresa no cuenta con recursos para miticar estos riesgos.

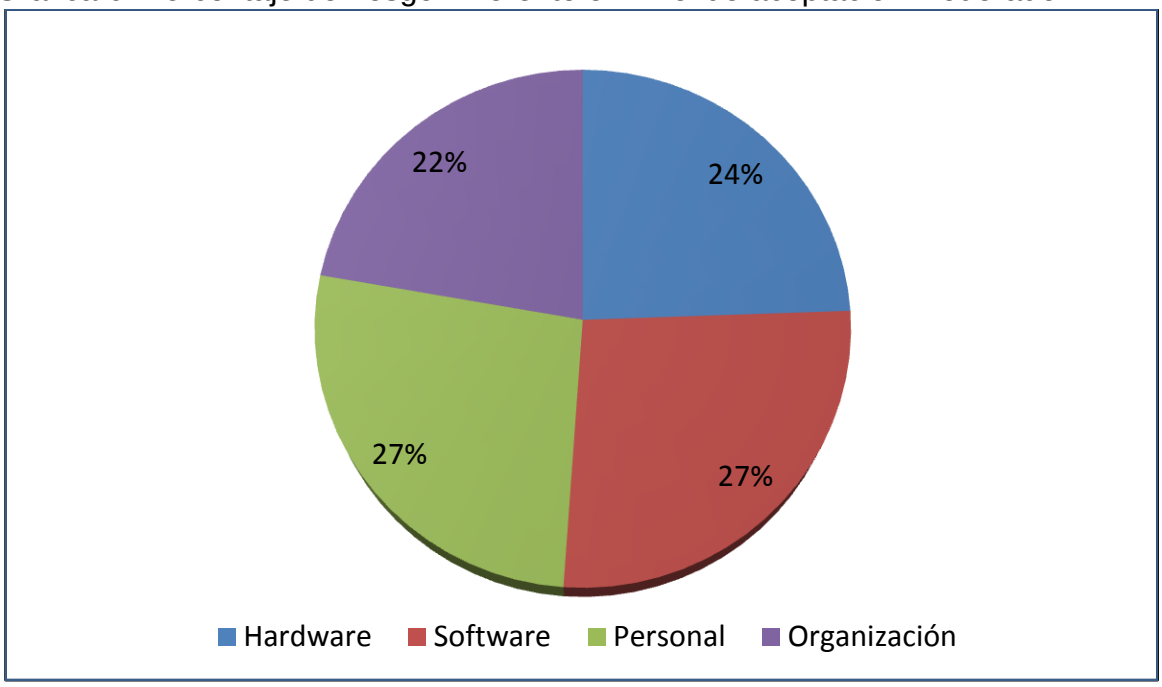
Posteriormente en el cuadro 13 se muestran los riesgos que tienen un nivel de aceptación “Moderado” es decir, que se encuentran dentro del rango de valor de aceptación 5–14, en un total de 8 riesgos; se publican en el anexo B (Matriz de resultados):

Cuadro 13. Riesgos en nivel de aceptación moderado.

Id	Tipo de activo	Vulnerabilidad	Amenaza	Riesgos (inherente)	Nivel de aceptación
1	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Daños por polvo.	8	Moderado
2		Susceptibilidad a las variaciones de tensión.	Pérdida de suministro de energía.	12	Moderado
3		Almacenamiento sin protección.	Hurto de medios, documentos o equipos.	12	Moderado
4		Descarga y uso no controlados de software.	Manipulación con Software.	12	Moderado
5	Software	Falta de mecanismos de identificación y Autentificación.	Uso no autorizado del equipo.	12	Moderado
6	Personal	Uso incorrecto de software y hardware.	Abuso de derechos.	12	Moderado
7	Organización	Falta de procedimiento formal para la autorización de la información disponible al público.	Divulgación.	12	Moderado
8		Falta de política formal sobre la utilización de Computadores portátiles.	Hurto de equipo.	8	Moderado

Fuente: Elaboración autores.

Gráfica 6. Porcentaje de riesgo inherente en nivel de aceptación moderado.



Fuente: Elaboración autores.

De acuerdo al nivel de riesgo inherente para los tipos de activos con el nivel de aceptación moderado, se muestran con un mayor porcentaje el tipo de activo software y tipo personal como se visualizan en la gráfica 6, debido a que la organización actualmente no cuenta con mecanismos de identificación y autenticación para tener acceso al sistema, lo cual permite que los funcionarios del área de desarrollo pueden acceder a los equipos sin mayor restricción corriendo el riesgo de afectar la disponibillidad, integridad y confidencialidad de la información.

4.4 CONTROLES EXISTENTES

Como se sugiere en la norma ISO/IEC 27005 numeral 8.2.1.4 se deben de identificar los controles existentes para evitar trabajo y costos innecesarios, por ejemplo duplicación de los controles.

A continuación en el cuadro 14 se muestran los 10 controles existentes que se identificaron en el área de desarrollo de la organización.

Cuadro 14. Controles existentes.

Id	Control existente	Control equivalente en la norma ISO 27001	Descripción
1	Políticas de seguridad.	A.5.1.1 Políticas para la seguridad de la información.	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
2	Restricciones de la red para los dispositivos móviles.	A.6.2.1 Política para dispositivos móviles.	Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
3	Estudio del personal a contratar.	A.7.1.1 Selección.	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a la que se va a tener acceso, y a los riesgos percibidos.
4	Inventario de los activos de la empresa.	A.8.1.1 Inventario de activos.	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos**.**
5	Terminado el contrato con el empleado se devuelven los activos que fueron entregados inicialmente.	A.8.1.4 Devolución de activos.	Todos los empleados y usuarios de partes externas deben devolver todos los activos que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
6	Información clasificada por cada área.	A.8.2.1 Clasificación de la información. .	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Cuadro 14. (Continuación).

Id	Control existente	Control equivalente en la norma ISO 27001	Descripción
7	Cada estación cuenta con contraseña para inicio de sesión y portabilidad del carnet.	A.9.1.1 Política de control de acceso.	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
8	Existe un control para usuarios autorizados a acceder a la red y los servicios en red.	A.9.1.2 Acceso a redes y a servicios en red.	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
9	Se tiene restricción a la información, ya que solo puede tener acceso el personal autorizado.	A.9.4.1 Restricción de acceso a información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
10	Generan copias de respaldo una vez al mes.	A.12.3.1 Controles contra códigos maliciosos.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

Fuente: Elaboración autores.

Para la evaluación de los controles existentes se utilizó el cuadro 15 que fue definido mediante inspección directa en el área de desarrollo de la organización.

Cuadro 15. Calificación del control.

Cuantitativo	Cualitativo	Detalle
1	No existe	No existe el control.
2	Bajo	El control disminuye el riesgo con un porcentaje bajo estando inferior o igual a un veinte (20) porciento.
3	Medio	El control disminuye el riesgo con un porcentaje medio estando inferior o igual a un cuarenta (40) porciento.
4	Bueno	El control disminuye el riesgo con un porcentaje bueno estando inferior o igual a un ochenta (80) porciento.
5	Excelente	El control disminuye el riesgo con un porcentaje excelente estando superior a un ochenta (80) porciento.

Fuente: Elaboración autores.

La métrica de la calificación del control nos permite evaluar qué tan eficaz es el control para reducir el riesgo. Una forma de estimar el efecto del control es ver la manera en que reduce la probabilidad de ocurrencia de la amenaza y la facilidad de explotar la vulnerabilidad o el impacto del incidente.

4.5 CÁLCULO DEL RIESGO RESIDUAL

El excedente del riesgo inherente al aplicar sobre un control, es llamado riesgo residual y se calcula mediante la siguiente fórmula**.**

Riego residual = riesgo inherente / valoración del control.

Lo anterior se evidencia en el Anexo A del presente proyecto.

5. PROPUESTA PLAN DE GESTIÓN DE RIESGO OPERATIVO PARA EL ÁREA DE DESARROLLO

El objetivo del plan de gestión de riesgos consiste en reducir los riesgos de la organización, los cuales se muestran en la matriz de resultados, Anexo A, y se visualizan en la Gráfica 4 “Valoración de los riesgos”, donde se muestran los riesgos con nivel inaceptable en 62% y 38% moderado.

El plan de gestión de riesgos se realiza aplicando controles sugeridos con el objetivo de minimizar los riesgos que se evidencian en el proceso de evaluación de riesgos, los cuales se muestran en el Cuadro 12. “Riesgos en nivel inaceptable” y Cuadro 13 “Riesgos en nivel de aceptación moderado”.

Con respecto a lo anterior es pertinente contextualizar los controles sugeridos en el presente proyecto con la situación específica de la empresa.

El plan de gestión de riesgo contempla 4 fases:

- Fase 1. Identificación de los controles requeridos para cada riesgo: Se deben identificar los perfiles de los funcionarios que podrán implementar los controles para los riesgos ubicados en el cuadro 12 “Riesgos en nivel inaceptable” y Cuadro 13 “Riesgos en nivel de aceptación moderado”. En la matriz de resultados (Anexo A), se evalúa la relación directa entre cada riesgo y los controles sugeridos.

- Fase 2. El cálculo del valor de Costo – Beneficio: Se deberán asignar tres valores para la valoración de cada control: el primero de acuerdo al costo de implementación, el segundo de acuerdo a tiempo de implementación y por último, la valoración del incidente en el caso de que no se implemente dicho control.

- Fase 3. Presupuesto de implementación: Se calcula el valor de la implementación de cada uno de los controles en función del tiempo sugerido y de la complejidad.

- Fase 4. Cronograma para implementar el plan de gestión de riesgos. Se muestra el tiempo propuesto que llevara a cada funcionario implementar los controles sugeridos.

5.1 IDENTIFICACIÓN DE LOS CONTROLES REQUERIDOS PARA CADA RIESGO.

Para llevar a cabo la implementación del plan de gestión de riesgos se sugiere un tiempo y un perfil definido en el cuadro 16 para la ejecución de cada control.

Cuadro 16. Descripción de cargos.

Id	Cargo	Perfil
1	Ingeniero de sistemas.	Desarrollador de software, con experiencia en manejo de sistemas operativos Windows y Linux, destrezas en configuración de firewall. Experiencia mínimo de 2 años.
2	Especialista en seguridad informática.	Con experiencia en gestión de riesgos, habilidades para dictar capacitaciones en temas relacionados a la seguridad informática, generación de políticas y procedimientos de seguridad, y elaboración de planes de continuidad. Experiencia mínimo de 2 años.
3	Técnico en sistemas.	Con experiencia en mantenimiento de equipos de cómputo y en instalaciones de sistemas de vigilancia.
4	Jefe de recursos humanos	Experiencia en coordinador de gestión humana, coordinar procesos, selección de personal, elaboración de contratos y cláusulas de permanencia. Experiencia mínimo de 1 año.

Fuente: Elaboración autores.

A continuación se describen los controles sugeridos para la implementación del plan de gestión de riesgos.

- **A.5.1.1 Documento de la política de seguridad de la información**.

Descripción: Documento de políticas de seguridad de la información, debe ser aprobado por la dirección de la organización. Este documento se debe publicar y comunicar a todos los funcionarios y demás áreas externas relacionadas con la organización.

Aplicación: Generar una política de seguridad de la información del uso adecuado de los computadores de la empresa, contando con el respaldo de la alta gerencia.

Persona a cargo: Especialista en Seguridad informática.

Tiempo estimado: 5 días.

- **A.6.1.3 Asignación de responsabilidades para la seguridad de la información.**

Descripción: En este control se deben de asignar claramente las responsabilidades de acuerdo a la seguridad de la información. Es muy importante que se establezcan de forma clara, teniendo en cuenta a todos los jefes de cada área.

Aplicación: Asignar un especialista en seguridad de la información que tendrá la responsabilidad general por el desarrollo e implementación de la seguridad y apoyar la identificación, implementación y reasignación de los controles. Asignar un jefe por cada área que tendrá las responsabilidades por cada recurso de información de manera permanente.

Persona a cargo: Especialista en Seguridad informática.

Tiempo de estimado: 5 días.

- **A.6.1.35 Acuerdos sobre confidencialidad.**

Descripción: Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de la organización.

Aplicación: Se deben establecer cláusulas de confidencialidad con los funcionarios de la organización, esto para que haya un mayor compromiso y mayor protección de la información sensible para la organización.

Persona a cargo: Jefe de recursos humanos.

Tiempo de ejecución: 5 días.

- **A.7.2.2 Etiquetado y manejo de información.**

Descripción: Se debe contar con procedimientos formales para el correcto etiquetado y manejo de información, ya sea físico o electrónico; utilizando el esquema de acuerdo a la clasificación anterior. Los procedimientos deben ser claros en cuanto a impresión, copiado, almacenamiento e intercambio.

Aplicación: se debe realizar un procedimiento para el etiquetado de información que abarque todos los activos de información en formatos electrónicos y físicos. Se debe tener en cuenta que la información crítica o sensible debe de tener el etiquetado apropiado, y unas reglas establecidas.

Cada nivel de clasificación, debe definir los procedimientos de manejo confiable, incluyendo el procesamiento para identificar la clasificación de la información.

Persona a cargo: Ingeniero de sistemas.

Tiempo de ejecución: 5 días.

- **A.8.2.1 Educación, formación y concientización sobre la seguridad de la información**.

Descripción: Todos los funcionarios de la organización externos e internos deben tener charlas, capacitaciones y actividades que les permita tomar conciencia de la importancia de la seguridad de la información.

Aplicación: Se debe iniciar en la organización un proceso de inducción formal, planificada y diseñada para introducir las políticas y expectativas de seguridad de la organización, antes de permitir acceso a los servicios o la información.
Las actividades deberían incluir requerimientos de seguridad, responsabilidades legales y controles, incluyendo el uso correcto de los medios de procesamiento de información como por ejemplo el uso de paquetes de software.

Persona a cargo: Especialista en seguridad informática.

Tiempo de ejecución: 3 días.

- **A.9.1.3 Seguridad de oficinas, recintos e instalaciones.**

Descripción: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.

Aplicación: Se recomienda la compra de guayas de seguridad para los computadores portátiles y la compra de cámaras de video para el área de desarrollo.

Persona a cargo de instalación: Técnico en Sistemas.

Tiempo de instalación: 5 días.

- **A.9.2.2 Servicios de suministro.**

Descripción: esporádicamente, la empresa se ve afecta por cortes de energía, donde se ve la necesidad de adquirir una planta eléctrica y una UPS como soporte, para evitar pérdidas de información y daños que pueden tener las estaciones de trabajo, esto impacta el desempeño laboral de los funcionarios de la empresa.

Aplicación: Se sugiere que la empresa adquiera una planta de energía eléctrica y una UPS.

Persona a cargo instalación: Técnico de sistemas.

Tiempo de Instalación: 5 días.

- **A.9.2.4 Mantenimiento de los equipos.**

Descripción: Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.

Aplicación: Se debe realizar mantenimiento a los equipos de cómputo periódicamente, para evitar daños ocasionados por humedad, polvo y suciedad, con el fin de asegurar su continua disponibilidad e integridad.

Persona a cargo: Técnico de sistemas.

Tiempo de ejecución: 5 días.

- **A.10.5.1 Respaldo de la información.**

Descripción: Se deben realizar procedimientos para extraer respaldos de la información importante para la organización.

Aplicación: Se debe realizar un procedimiento a seguir en el momento de realizar las copias de respaldo de la información, las cuales deben de ser validadas por el personal encargado. Se sugiere que la información sensible de la organización debe ser cifrada.

Persona a cargo: Ingeniero de sistemas.

Tiempo de ejecución: 15 días.

- **A.10.8.1 Políticas y procedimientos para el intercambio de información.**

Descripción: Se deben establecer políticas, procedimientos y controles formales de intercambio de información para proteger la información mediante el uso de todo tipo de servicios de comunicación.

Aplicación: se deben definir políticas y establecer procedimientos para el intercambio de la información. Se debe aplicar un mayor control a la información que sea más sensible para la organización.

Persona a cargo: Especialista en seguridad informática.

Tiempo de ejecución: 5 días.

- **A.10.10.2 Monitoreo del uso del sistema.**

Descripción: Se deben de realizar procedimientos para monitorear las acciones realizadas por los funcionarios en los sistemas de información de la organización.

Aplicación: Se sugiere adquirir un firewall y configurar las reglas adecuadas para permitir los accesos a los servicios a solo los funcionarios que los tengan permitidos, esto para evitar el uso inadecuado no autorizado.

Persona a cargo: Ingeniero de sistemas.

Tiempo de instalación: 10 días.

- **A.11.2.2 Gestión de privilegios.**

Descripción: Se debe restringir y controlar la asignación y uso de privilegios.

Aplicación: Se debe realizar un proceso de autorización formal, donde se controle la asignación de privilegios de acuerdo a cada producto del sistema como por ejemplo el sistema operativo, base de datos y cada aplicativo; identificando cada funcionario que necesite que se le asignen privilegios.

Persona a cargo: Ingeniero de sistemas.

Tiempo de estimado: 5 días.

- **A.11.5.2 Identificación y autenticación de usuarios.**

Descripción: Este control se refiere a que todos los usuarios deben de tener un identificador único, propio para su uso personal y exclusivo, para así poder comprobar la identidad del usuario.

Aplicación: Se debe realizar una política de seguridad, e implementar un proceso donde se establezca que todo funcionario debe de tener un usuario único en la red corporativa.

Persona a cargo: Ingeniero de Sistemas.

Tiempo de ejecución: 5 días.

- **A.11.5.5 Tiempo de inactividad de la sesión.**

Descripción: Las sesiones inactivas se deben suspender después de un periodo definido de inactivación.

Aplicación: Se debe establecer un proceso el cual después de cierto tiempo en que la sesión se encuentre inactiva, evite el uso no autorizado de personas y la negación de ataques de servicios.

Persona a cargo: Ingeniero de sistemas.

Tiempo de estimado: 5 días.

- **A.14.1.2 Continuidad del negocio y evaluación de riesgos.**

Descripción: Se debe identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

Aplicación: Se deben documentar todos los incidentes que ocasionan interrupciones en la organización y sus consecuencias con respecto a la seguridad de la información. Esto es necesario para poder realizar un plan de continuidad del negocio.

Persona a cargo: Especialista en seguridad informática.

Tiempo de ejecución: 10 días.

- **A.14.1.3 Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información.**

Descripción: Se deben desarrollar planes que permitan mantener y restaurar las operaciones de la organización, asegurando la disponibilidad de la información del área de desarrollo.

Aplicación: Generar planes de continuidad del negocio donde se identifiquen todas las responsabilidades y los procedimientos del negocio.

Persona a cargo: Especialista en seguridad informática.

Tiempo de ejecución: 10 días.

5.2 CÁLCULO DEL VALOR COSTO – BENEFICIO

Se deberán asignar tres valores para la valoración de cada control: el primero de acuerdo al costo de implementación, el segundo de acuerdo al tiempo de implementación y por último, la valoración del incidente en el caso de que no se implemente dicho control.

A continuación en el cuadro 17 se muestran las métricas para el costo de implementación.

Cuadro 17. Costo de implementación.

Valor cuantitativo	Valor cualitativo	Detalle
1	Menor	Menor a un SMMLV
2	Bajo	De 1 a 5 SMMLV
3	Medio	De 5 a 10 SMMLV
4	Alto	De 15 a 20 SMMLV
5	Muy Alto	Mayor a 20 SMMLV

Fuente: Elaboración autores.

El costo de implementación de la información se relaciona en el cuadro 17 ya que permite identificar el valor promedio que costara implementar cada control.

Se mencionan las métricas del tiempo de implementación descritas en el cuadro 18:

Cuadro 18. Tiempo de implementación.

Valor cuantitativo	Valor cualitativo	Descripción
1	Menor	1 a 3 días
2	Bajo	Inferior a 4semanas.
3	Medio	Inferior a 10 semanas.
4	Alto	Inferior a 15 semanas.
5	Muy alto	Superior a 20 semanas.

Fuente: Elaboración autores.

A través de las métricas del tiempo de implementación se puede valorar y estimar el tiempo promedio para la implementación del control.

A continuación en el cuadro 19 se relaciona las métricas de valoración de cada incidente si no se implementa el control.

Cuadro 19. Valoración de un incidente si no se implementa el control.

Valor	Impacto	Descripción
1	Insignificante	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas insignificantes en el incumplimiento de la legislación y/o reglamentación, deterioro en el desempeño del negocio, pérdidas financieras o pérdida del buen nombre de la organización.
2	Bajo	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas bajas en el incumplimiento de la legislación y/o reglamentación, deterioro en el desempeño del negocio, pérdidas financieras o pérdida del buen nombre de la organización.
3	Moderado	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas moderadas en el incumplimiento de la legislación y/o reglamentación, deterioro en el desempeño del negocio, pérdidas financieras o pérdida del buen nombre de la organización.
4	Alto	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas altas en el incumplimiento de la legislación y/o reglamentación, deterioro en el desempeño del negocio, pérdidas financieras o pérdida del buen nombre de la organización.
5	Extremo	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas totales en el incumplimiento de la legislación y/o reglamentación, deterioro en el desempeño del negocio, pérdidas financieras o pérdida del buen nombre de la organización.

Fuente: Elaboración autores.

Como se definió en el cuadro 19 la valoración del incidente en caso de no implementarse el control se realiza teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información.

Se evalúa el costo–beneficio de la siguiente forma:

Costo-beneficio = (costo de implementación +tiempo de implementación +valoración de incidente) / 3.

A continuación en el cuadro 20 se muestran las métricas para la valoración del costo-beneficio.

Cuadro 20. Valoración Costo – Beneficio.

Valor	Descripción
1	No se implementa el control.
2	El costo – Beneficio tiene un valor bajo.
3	El costo – Beneficio tiene un valor medio.
4	El costo – Beneficio tiene un valor alto.
5	El costo – Beneficio tiene un valor muy alto.

Fuente: Elaboración autores.

Los valores definidos en el cuadro 20 dan una referencia del costo y el beneficio que se tendrá al implementar cada control sugerido.

5.3 PRESUPESTO DE IMPLEMENTACIÓN

En el plan de gestión de riesgos se encuentran los diversos controles que se deben implementar para la empresa en estudio. En el presente ítem se calcula el valor de cada uno de ellos en función del tiempo y de la complejidad, como también si el recurso final constituye hardware, software, documento, manual y quién es el profesional que debe realizarlo, como se definieron en el cuadro 21:

Cuadro 21. Presupuesto de implementación.

Id	Control norma ISO 27001	Tipo	Recurso	Descripción del software y/o hardware	Cantidad	Unidad de medida	Valor unitario	Subtotal
1	A.5.1.1	Documento	Especialista en seguridad informática.		5	día/s	200,000	1,000,000
2	A.6.1.3	Documento	Especialista en seguridad informática.		5	día/s	200,000	1,000,000
3	A.6.1.5	Documento	Jefe de recursos humanos.		5	día/s	125,000	625,000
4	A.7.2.2	Manual de procedimientos	Ingeniero de sistemas.		5	día/s	100,000	500,000
5	A.8.2.1	Capacitación	Especialista en seguridad informática.		3	día/s	200,000	600,000
6	A.9.1.3	Instalación	Técnico en sistemas.		5	día/s	40,000	200,000
7	A.9.1.3	Elemento de seguridad	Guaya.	Guaya Para Portátil Alta Seguridad X-kim X-safe Profesional	2	Unidad	30,000	60,000
8	A.9.1.3	Hardware	Cámaras de vigilancia.	Kit Completo Video Vigilancia Cctv Dvr 8 Canales + 4 Cámaras.	1	Unidad	450,000	450,000
9	A.9.2.2	Instalación	Técnico en sistemas		5	día/s	40,000	200,000

Cuadro 21. (Continuación).

Id	Control norma ISO 27001	Tipo	Recurso	Descripción del software y/o hardware	Cantidad	Unidad de medida	Valor unitario	Subtotal
10	A.9.2.2	Hardware	Planta eléctrica	Planta Eléctrica Gene rador Honda E 6000x	1	Unidad	2,800.000	2,800.000
11	A.9.2.2	Hardware	ups	Ups Doble Conversión Smart online 1.5kva Torre Tripp-lite	1	Unidad	1,900,000	1,900,000
12	A.9.2.4	Mantenimiento	Técnico en sistemas		5	día/s	40,000	200,000
13	A.10.5.1	Procedimiento	Ingeniero de sistemas		15	día/s	100,000	1,500,000
14	A.10.8.1	Documento políticas y procedimientos	Especialista en seguridad		5	día/s	200,000	1,000,000
15	A.10.10.2	Hardware	Firewall	Router Inalámbrico Cisco Rv120w-a-na, Para 5 Vpn Y Firewall	1	Unidad	585,000	585,000
16	A.10.10.2	Instalación	Ingeniero de sistemas		10	día/s	100,000	1,000,000
17	A.11.2.2	Procedimiento	Ingeniero de sistemas		5	día/s	100,000	500,000
18	A.11.5.2	Procedimiento	Ingeniero de sistemas		5	día/s	100,000	500,000
19	A.11.5.5	Procedimiento	Ingeniero de sistemas		5	día/s	100,000	500,000
20	A.14.1.2	Documento	Especialista en seguridad		10	día/s	200,000	2,000,000
21	A.14.1.3	Documento	Especialista en seguridad		10	día/s	200,000	2,000,000
	VALOR TOTAL							19,120,000

Fuente: Elaboración autores.

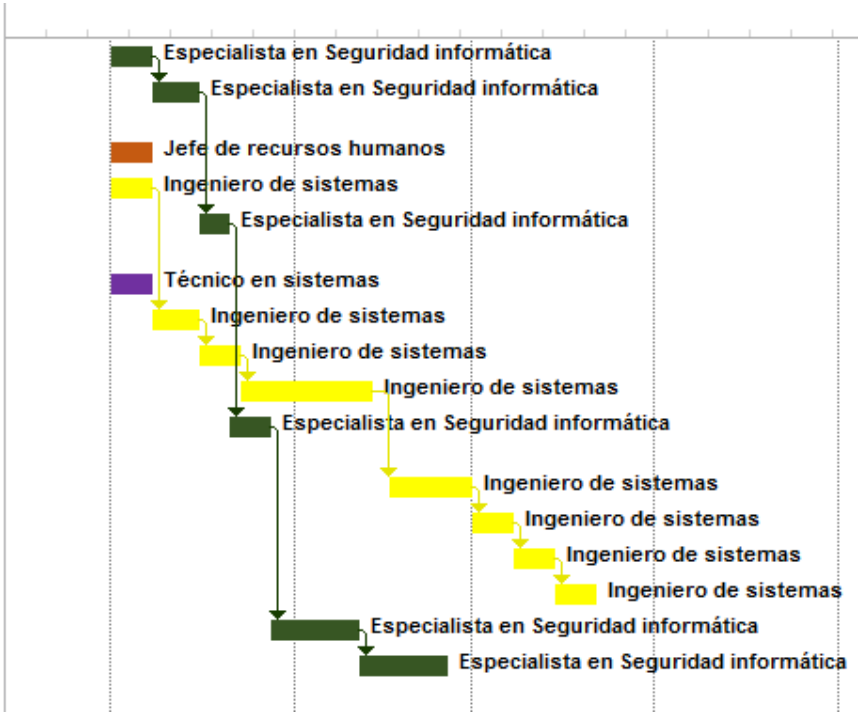
De acuerdo al cuadro 21 como resultado estimado del presupuesto para realizar el plan de gestión de riesgos para el área de desarrollo de la empresa VYG Tecnología y Soluciones es de $19,120,000.

5.4 CRONOGRAMA PARA LA IMPLEMENTACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Se relaciona en la gráfica 7 el cronograma para la implementación del plan de gestión de riesgos de acuerdo a los tiempos propuestos de cada control.

Gráfica 7. Cronograma para la implementación del plan de gestión de riesgos.

Nombre de tarea	Duración
A.5.1.1 Documento de la política de seguridad de la información.	5 días
A.6.1.3 Asignación de responsabilidades para la seguridad de la información	5 días
A.6.1.5 Acuerdos sobre confidencialidad	5 días
A.7.2.2 Etiquetado y manejo de información	5 días
A.8.2.1 Educación, formación y concientización sobre la seguridad de la información	3 días
A.9.1.3 Seguridad de oficinas, recintos e instalaciones	5 días
A.9.2.2 Servicios de suministro	5 días
A.9.2.4 Mantenimiento de los equipos.	5 días
A.10.5.1 Respaldo de la información	15 días
A.10.8.1 Políticas y procedimientos para el intercambio de información	5 días
A.10.10.2 Monitoreo del uso del sistema	10 días
A.11.2.2 Gestión de privilegios	5 días
A.11.5.2 Identificación y autenticación de usuarios.	5 días
A.11.5.5 Tiempo de inactividad de la sesión	5 días
A.14.1.2 continuidad del negocio y evaluación de riesgos	10 días
A.14.1.3 Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	10 días



Fuente: Elaboración autores.

El tiempo estimado de implementar el plan de gestión de riesgos sería aproximadamente de 3 meses.

6. ANÁLISIS DE RESULTADOS

Para el análisis de resultados, se individualizó los aspectos más importantes, distribuidos de la siguiente forma:

6.1 VULNERABILIDADES CON MAYOR NÚMERO DE INCIDENCIAS

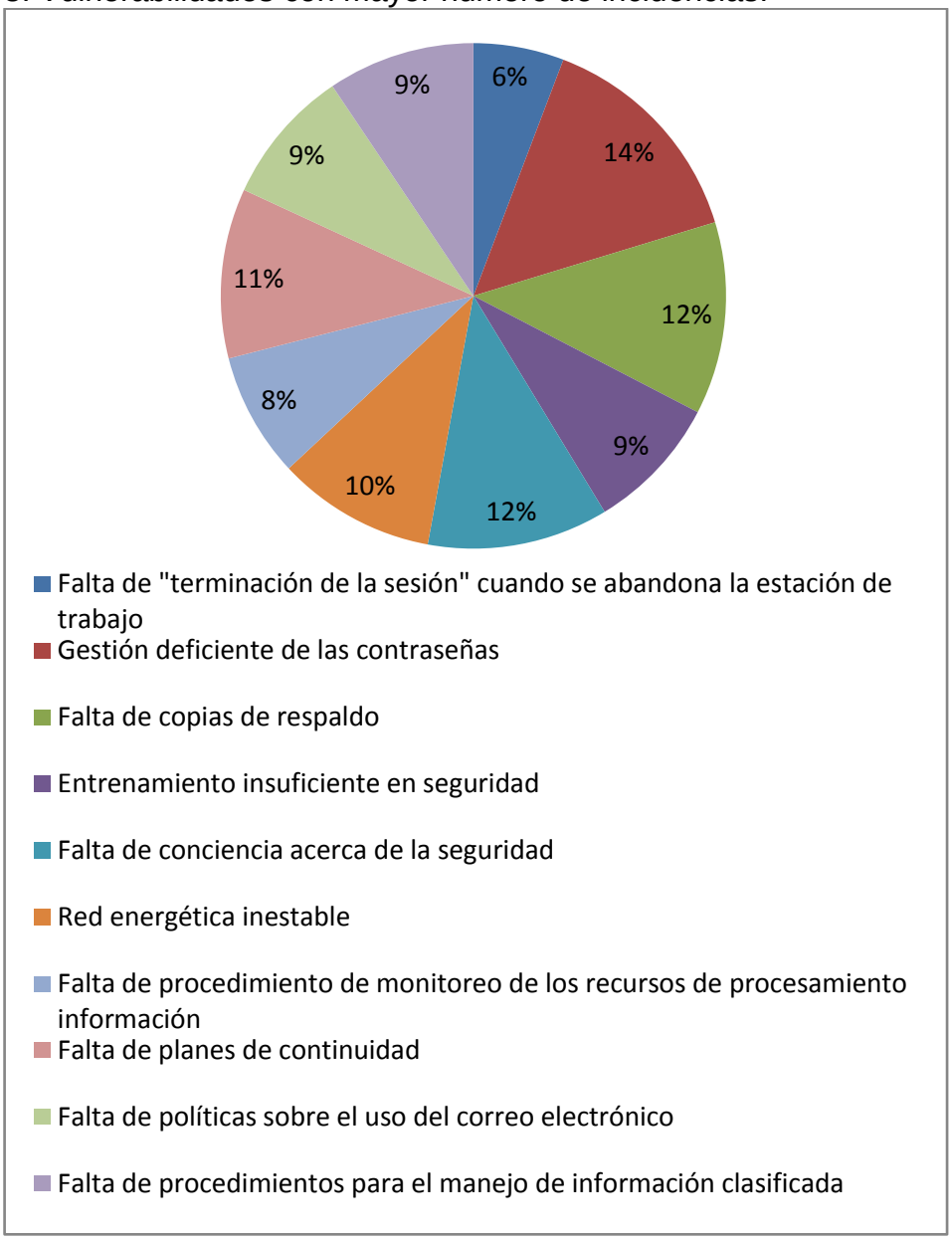
De las 21 vulnerabilidades identificadas, a continuación en el cuadro 22 se enuncian las 10 vulnerabilidades con mayor número de incidencias en la empresa:

Cuadro 22. Vulnerabilidades con mayor número de incidencias.

Id	Vulnerabilidades	Número de incidencias
1	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	8
2	Gestión deficiente de las contraseñas	20
3	Falta de copias de respaldo	17
4	Entrenamiento insuficiente en seguridad	12
5	Falta de conciencia acerca de la seguridad	16
6	Red energética inestable	14
7	Falta de procedimiento de monitoreo de los recursos de procesamiento información	11
8	Falta de planes de continuidad	15
9	Falta de políticas sobre el uso del correo electrónico	12
10	Falta de procedimientos para el manejo de información clasificada	13

Fuente: Elaboración autores.

Gráfica 8. Vulnerabilidades con mayor número de incidencias.



Fuente: Elaboración autores.

De acuerdo a la información de la gráfica 8 se observa que las principales vulnerabilidades son: en primer lugar, gestión deficiente de las contraseñas (14%), esto se debe a que en la organización no existen los controles y/o políticas adecuadas para el acceso a los sistemas de información. En segundo lugar, falta de copias de respaldo (12%), los empleados del área de infraestructura no tienen un procedimiento para realizar copias de respaldo de la información. Y en tercer

lugar, falta de conciencia acerca de la seguridad (12%), esto se debe a la usencia de capacitaciones, charlas, videos y juegos relacionados con la importancia de seguridad en la información en el área de desarrollo y en la empresa.

6.2 AMENAZAS CON MAYOR NÚMERO DE INCIDENCIAS

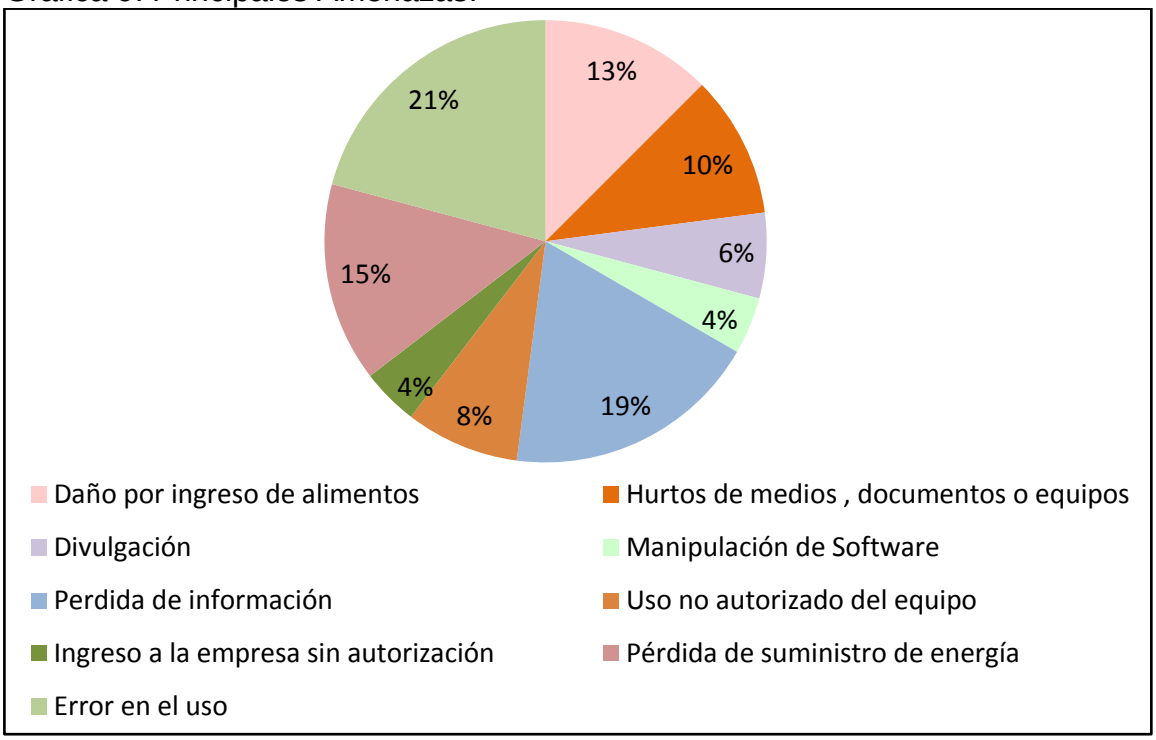
De las 14 amenazas detectadas, a continuación en el cuadro 23 se muestran las 10 principales que afectan los procesos del área de desarrollo de la organización, al igual que el número de incidencias presentadas por cada amenaza.

Cuadro 23. Número de incidencias por cada amenaza.

No	Amenazas	Número de incidencias
1	Daño por ingreso de alimentos	6
2	Hurtos de medios , documentos o equipos	5
3	Divulgación	3
4	Manipulación de Software	2
5	Perdida de información	9
6	Uso no autorizado del equipo	4
7	Ingreso a la empresa sin autorización	2
8	Pérdida de suministro de energía	7
9	Error en el uso	10
10	Abuso de derechos	4

Fuente: Elaboración autores.

Gráfica 9. Principales Amenazas.



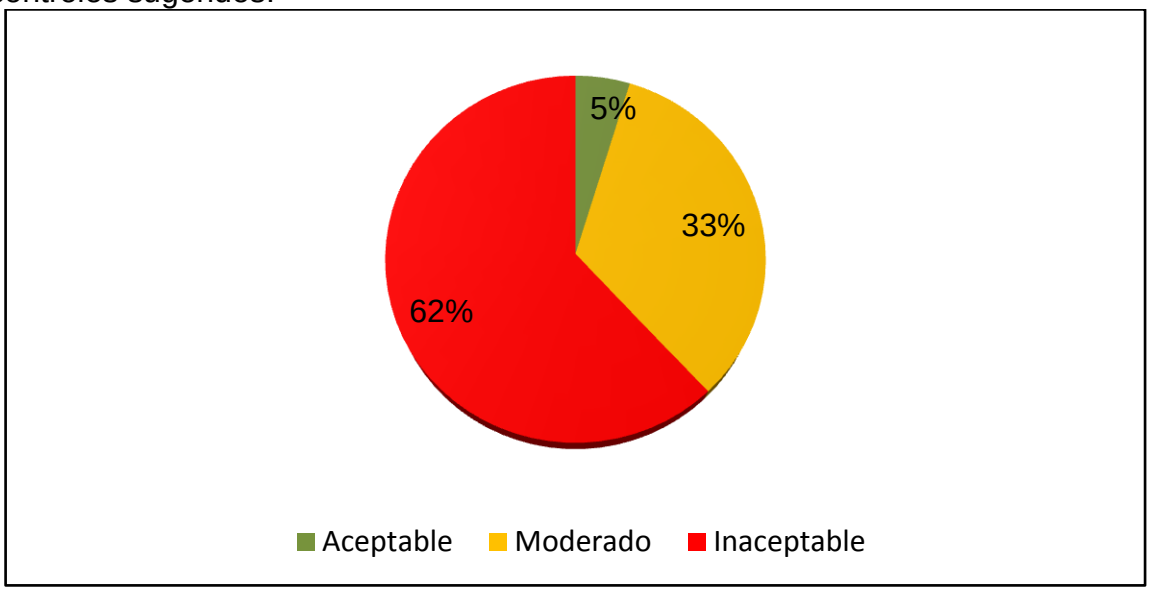
Fuente: Elaboración autores.

Como resultado se observa en la gráfica 9 que las principales amenazas que afectan e impactan el área de desarrollo son: primero, error en el uso (21%). Se debe a que no existe un procedimientos, ni documentación para el manejo de la información con temas relacionados con la seguridad de la información, en segundo lugar perdida de información (19%), en la empresa no existe un procedimiento para realizar copias de respaldo de la información, y tercer lugar, perdida de suministro de energía (15%), se evidencia que la empresa no esta preparada para controlar la perdida de energía por un lapso de tiempo, afectando los objetivos del negocio.

6.3 VALORACIÓN DE RIESGO

En la siguiente gráfica se visualiza el porcentaje de riesgos antes de la implementación de los controles sugeridos.

Gráfica 10. Porcentaje de nivel de aceptación de riesgos antes de implementar controles sugeridos.



Fuente: Elaboración autores.

Como se aprecia en la gráfica 10 más de la mitad de los riesgos hallados (62%) en los procesos en estudio se encuentra en la zona inaceptable de acuerdo a la valoración realizada para el presente proyecto y el (38%) restante están en la zona aceptable y moderada, se determinó evaluar y tratar todos los riesgos ya que actualmente la empresa tiene bajo nivel de seguridad en el área de desarrollo y tiene implementados pocos controles, y la mayoría son ineficientes.

6.4 CONTROLES MÁS SUGERIDOS

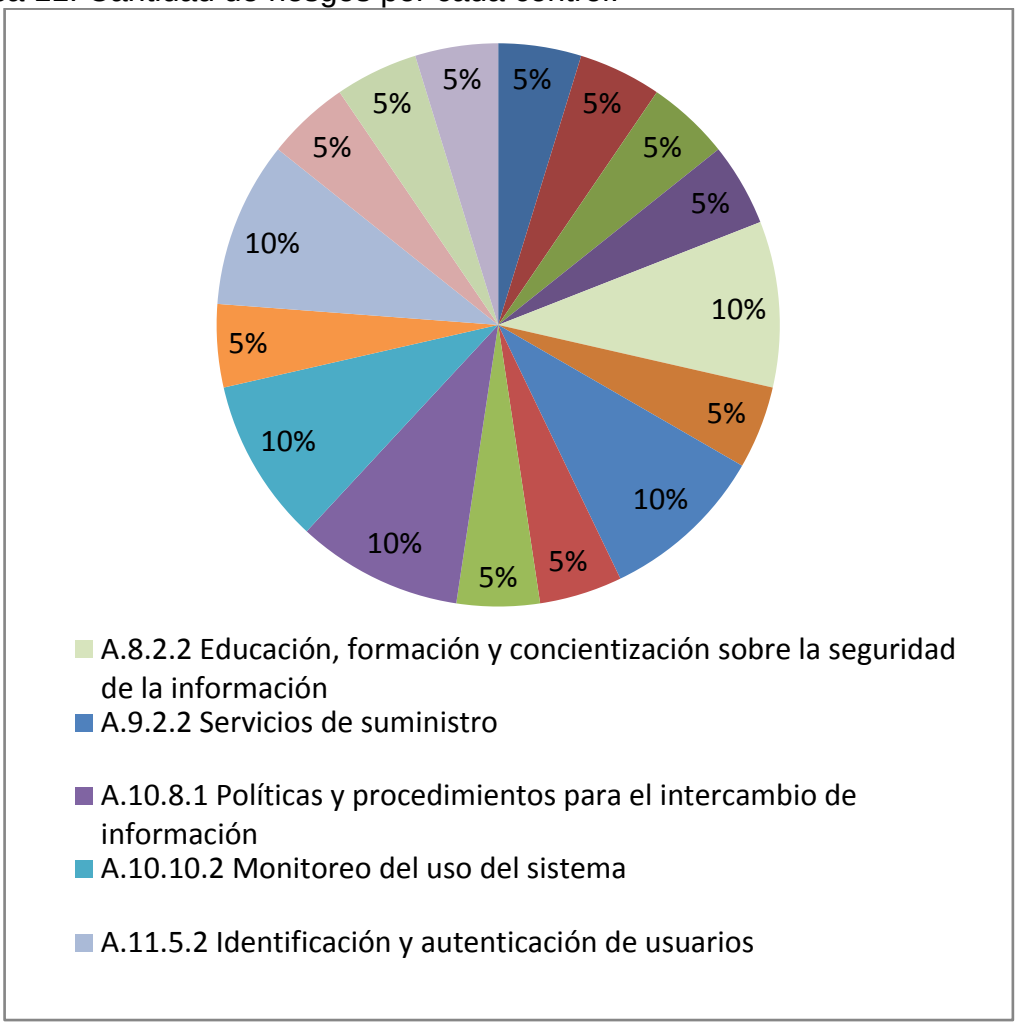
De acuerdo a la norma ISO/IEC 27001 en su anexo A, se precisaron 16 controles para 21 vulnerabilidades y 14 amenazas los cuales se mencionan en el cuadro 24 en relación a la cantidad de riesgos que aplica cada control.

Cuadro 24. Principales Controles.

Id	Norma ISO 27001	Controles sugeridos	Cantidad de riesgos que aplica el control
1	A.5.1.1	Documento de la política de seguridad de la información.	1
2	A.6.1.3	Asignación de responsabilidades para la seguridad de la información.	1
3	A.6.1.5	Acuerdos sobre confidencialidad.	1
4	A.7.2.2	Etiquetado y manejo de información.	1
5	A.8.2.2	Educación, formación y concientización sobre la seguridad de la información.	2
6	A.9.1.3	Seguridad de oficinas, recintos e instalaciones.	1
7	A.9.2.2	Servicios de suministro.	2
8	A.9.2.4	Mantenimiento de los equipos.	1
9	A.10.5.1	Respaldo de la información.	1
10	A.10.8.1	Políticas y procedimientos para el intercambio de información.	2
11	A.10.10.2	Monitoreo del uso del sistema.	2
12	A.11.2.2	Gestión de privilegios.	1
13	A.11.5.2	Identificación y autenticación de usuarios.	2
14	A.11.5.5	Tiempo de inactividad de la sesión	1
15	A.14.1.2	continuidad del negocio y evaluación de riesgos	1
16	A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	1

Fuente: Elaboración autores.

Gráfica 11. Cantidad de riesgos por cada control.



Fuente: Elaboración autores.

Se observa en la gráfica 11 que los controles con mayor número de riesgos fueron 5, cada uno aplicando un 10% del total de los riesgos encontrados en la evaluación de riesgos.

- El control A.8.2.2 Educación, formación y concientización sobre la seguridad de la información. Este control le va a permitir a la empresa mitigar el riesgo de error humano ya que los funcionarios tendrían un mayor conocimiento con respecto a la importancia de la seguridad de la información en la organización.

- El control A.9.2.2 Servicios de suministros. En la empresa se presentan inconvenientes afectando el suministro de energía, ocasionando fallas en los equipos, pérdida de información, generando atraso en las actividades laborales.

- A10.8.1 políticas y procedimientos de intercambio de información. Se debe a que los empleados pueden extraer información sensible de la empresa por medio del correo electrónico.

- A.10.10.2 Monitoreo del uso del sistema. No existen procedimientos que permitan monitorear los recursos de procesamiento de la información.

- A.11.5.2 identificación y autenticación de usuarios. Este proceso no se realiza de manera correcta en la empresa, porque el área de infraestructura asigna las mismas contraseñas para todos los funcionarios del área de desarrollo, sin establecer un mecanismo de identificación y autenticación único para cada empleado.

6.5 COSTO-BENEFICIO

A continuación en el cuadro 25 se muestran los controles con bajo – costo beneficio.

Cuadro 25. Controles con bajo costo-beneficio.

Control	Costo-Beneficio
A.6.1.3 Asignación de responsabilidades para la seguridad de la información	2
A.7.2.2 Etiquetado y manejo de información	2
A.8.2.1 Educación, formación y concientización sobre la seguridad de la información	2
A.9.2.2 Servicios de suministro	2
A.10.8.1 Políticas y procedimientos para el intercambio de información	2
A.10.10.2 Monitoreo del uso del sistema	2
A.10.51 Respaldo de la información	2
A.11.5.2 Identificación y autenticación de usuarios	2
A.14.1.2 continuidad del negocio y evaluación de riesgos	2
A.14.1.3 Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	2

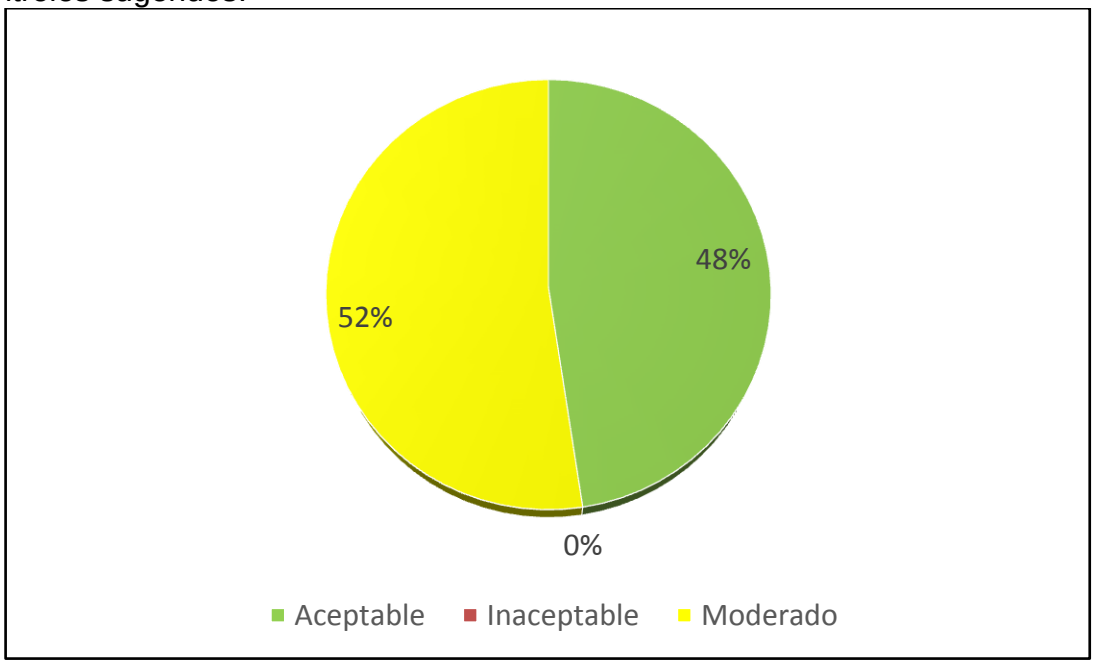
Fuente: Elaboración autores.

Los controles generan un beneficio alto a bajo costo, por lo tanto, se recomienda implementar dichos controles.

6.6 RESULTADO OBTENIDO DEL PLAN DE GESTIÓN DE RIESGOS

En la gráfica 12 se detalla el nivel de aceptación de los riesgos que quedaron como resultado del plan de gestión de riesgos.

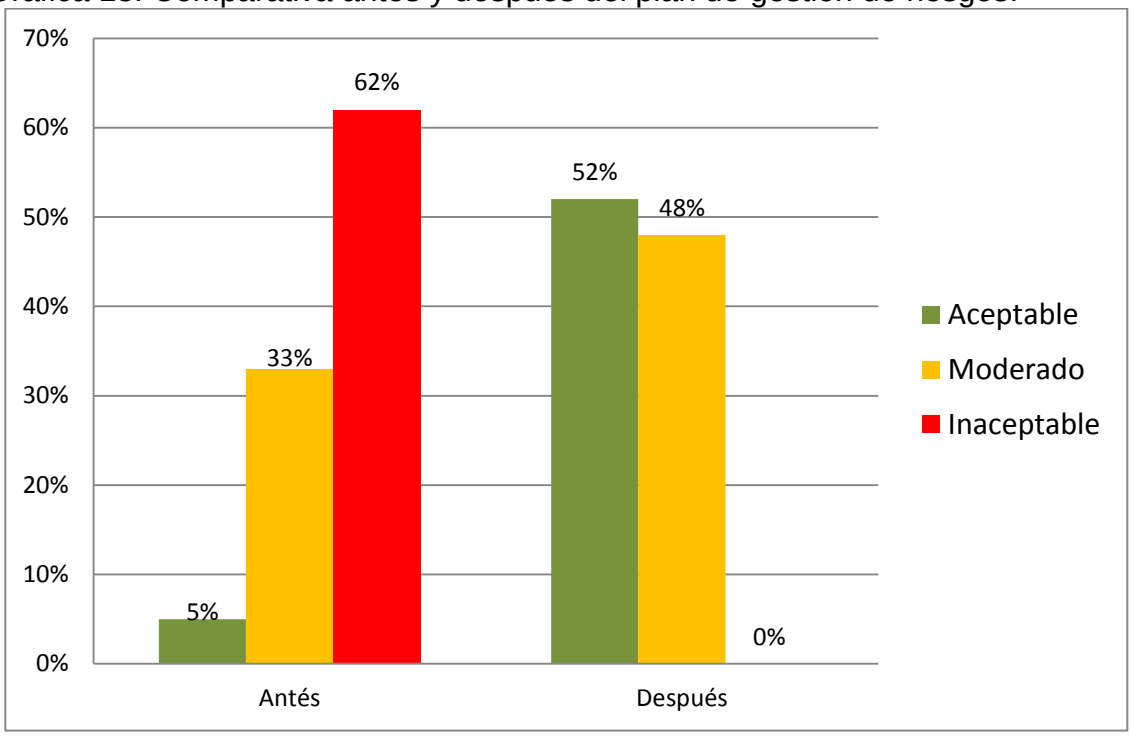
Gráfica 12. Porcentaje de nivel de aceptación de riesgos después de implementar controles sugeridos.



Fuente: Elaboración autores.

En lo que respecta a la mitigación del riesgo de un total de 62% de riesgos en el rango inaceptable, pasaron a (52%) a nivel moderado y de un total de 38% riesgos moderados, pasaron a 48% a nivel aceptable.

Gráfica 13. Comparativa antes y después del plan de gestión de riesgos.



Fuente: Elaboración autores.

Como se muestra en la gráfica 13 la mitigación del riesgo de un total de (62%) riesgos, en el rango inaceptable pasaron a (0%), de (33%) en nivel moderado pasaron a (48%) y de un total de (5%) riesgos en nivel aceptable, pasaron a (52%).

7. CONCLUSIONES

En la propuesta de un plan de gestión de riesgo operativo en el área de desarrollo de la empresa VYG tecnología y soluciones, al realizar el análisis, la evaluación y el tratamiento de riesgos se concluye:

Al hallar los riesgos residuales, se consideró que los controles existentes en la organización son insuficientes.

Al realizar el análisis del riesgo se detectaron 14 amenazas y 21 vulnerabilidades.

Se encontraron 205 activos para el área de desarrollo.

Las principales vulnerabilidades que presentan los activos son: gestión deficiente de las contraseñas (14%), falta de copias de respaldo (12%) y falta de conciencia acerca de la seguridad (12%).

El 5% de los riesgos se encuentran en el rango aceptable, el 33% en el rango moderado y el 62% de los riesgos se presentan como inaceptables.

En cuanto a controles, de acuerdo con la norma ISO/IEC 27001 en su anexo A, se precisaron 16 controles para 21 vulnerabilidades y 14 amenazas.

Los controles que aplican para un mayor número de riesgos son A.8.2.2 Educación, formación y concientización sobre la seguridad de la información (10%), A.9.2.2 Servicios de suministros, (10%), A10.8.1 políticas y procedimientos de intercambio de información (10%), A.10.8.1 Monitoreo del uso del sistema (10%), A.11.5.2 identificación y autenticación de usuarios (10%). Los controles anteriormente mencionados están de acuerdo a la norma ISO/IEC 27001:2005 en su anexo A.

En lo que respecta a la mitigación del riesgo de un total de (62%) de riesgos en el rango inaceptable pasaron a (0%), de (33%) en nivel moderado pasaron a (48%) y de un total de (5%) riesgos en nivel aceptable, pasaron a (52%) después de los controles sugeridos.

Si se implementa este plan de gestión de riesgos, la empresa VYG TECNOLOGÍA Y SOLUCIONES estará mejor preparada contra las amenazas que se presentan en la actualidad, logrando tener una mayor seguridad de la información.

8. BIBLIOGRAFIA

Administración del riesgo operacional en Colombia. consultado el 29 de Agosto de 2014. Disponible desde internet en: http://publicaciones.eafit.edu.co/index.php/administer/article/viewFile/553/499] pág.2, (consultado el 29 de agostos 2014).

INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Norma Técnica Colombiana para la Tecnología de la información, técnicas de seguridad de la información (SGSI), requisitos. Bogotá D.C, ICONTEC, 2006.NTC-ISO/IEC 27001.

INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Norma Técnica Colombiana para la Gestión de riesgo. Bogotá D.C, ICONTEC, 2008.NTC- 5254.

INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Norma Técnica Colombiana para la presentación de tesis, trabajos de grado y otros trabajos de investigación. Bogotá D.C, ICONTEC, 2008. NTC 1486.

INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Norma Técnica Colombiana para referencias documentales para fuentes de información electrónicas. Bogotá D.C, ICONTEC, 2008. NTC 4490.

INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Norma Técnica Colombiana para la presentación de tesis, trabajos de grado y otros trabajos de investigación. Bogotá D.C, ICONTEC, 2008. NTC 1486.

La gestión de riesgos se hace hueco en la agenda de las empresas, consultado el 15 de septiembre de 2014. http://www.elconfidencial.com/empresas/2014-01-30/la-gestion-de-riesgos-se-hace-hueco-en-la-agenda-de-las-empresas_82351.

UNAD. Investigación Exploratoria, Descriptiva, Correlacional y Explicativa Disponible desde internet en: http://datateca.unad.edu.co/contenidos/100104/100104_EXE/leccin_6_investigacin__exploratoria_descriptiva_correlacional_y_explicativa.html.

ANEXOS

Anexo A. Matriz de resultados.

Número	Activos	Vulnerabilidad	Amenaza	Impacto	Probabilidad de ocurrencia	Riesgos (inherente)	Control existente	Eficacia control existente	Riego residual para control existente	Nivel de aceptación del riesgo	Controles sugeridos	Tiempo de implementación [días]	Costo de implementación	Valoración de incidencia	Costo- beneficio	Riesgo residual para controles sugeridos	Nivel de aceptación del riesgo
1	HARDWARE	Susceptibilidad a la humedad, el polvo y la suciedad.	Daños por polvo.	4	2	8	Sin control	1	8	Moderado	A.9.2.4 Mantenimiento de los equipos.	5	1	2	3	3	Aceptable.
		Susceptibilidad a las variaciones de tensión	Pérdida de suministro de energía.	4	3	12	Sin control	1	12	Moderado	A.9.2.2 Servicios de suministro	5	3	4	4	3	Aceptable.
		Almacenamiento sin protección	Hurto de medios, documentos o equipos.	4	3	12	Sin control	1	12	Moderado.	A.9.1.3 Seguridad de oficinas, recintos e instalaciones.	5	2	3	3	4	Aceptable.
2	SOFTWARE	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	Uso no autorizado del equipo.	4	5	20	Sin control	1	20	Inaceptable.	A.11.5.5 Tiempo de inactividad de la sesión	5	1	2	3	7	Moderado.

Anexo A. (Continuación).

Número	Activos	Vulnerabilidad	Amenaza	Impacto	Probabilidad de ocurrencia	Riesgos (inherente)	Control existente	Eficacia control existente	Riego residual para control existente	Nivel de aceptación del riesgo	Controles sugeridos	Tiempo de implementación [días]	Costo de implementación	Valoración de incidencia	Costo- beneficio	Riesgo residual para controles sugeridos	Nivel de aceptación del riesgo
2	SOFTWARE	Falta de mecanismos de identificación y autentificación.		4	3	12	7	3	4	Aceptable	A.11.5.2 Identificación y autenticación de usuarios.	5	1	3	3	1	Aceptable
		Gestión deficiente de las contraseñas		4	5	20	Sin control	1	20	Inaceptable	A.11.5.2 Identificación y autenticación de usuarios.	5	1	3	3	7	moderado
		Descarga y uso no controlados de software.	Manipulación con Software.	4	3	12	Sin control	1	12	Moderado	A.11.2.2 Gestión de privilegios.	5	1	4	3	4	Aceptable
		Falta de copias de respaldo.	Pérdida de Información.	4	4	16	Sin control	1	16	Inaceptable	A.10.5.1 Respaldo de la información.	15	2	4	7	2	Aceptable

Anexo A. (Continuación).

Número	Activos	Vulnerabilidad	Amenaza	Impacto	Probabilidad de ocurrencia	Riesgos (inherente)	Control existente	Eficacia control existente	Riego residual para control existente	Nivel de aceptación del riesgo	Controles sugeridos	Tiempo de implementación [días]	Costo de implementación	Valoración de incidencia	Costo- beneficio	Riesgo residual para controles sugeridos	Nivel de aceptación del riesgo
3	PERSONAL	Entrenamiento insuficiente en seguridad.	Abuso de derechos.	4	4	16	Sin control	1	16	Inaceptable	A.8.2.1 Educación, formación y concientización sobre la seguridad de la información.	3	1	3	2	8	Moderado
		Uso incorrecto de software y hardware.		4	3	12	Sin control	1	12	Moderado	A.10.10.2 Monitoreo del uso del sistema.	10	1	4	5	2	Aceptable
		Falta de conciencia acerca de la seguridad.		4	4	16	Sin control	1	16	Inaceptable	A.8.2.2 Educación, formación y concientización sobre la seguridad de la información.	3	1	3	2	8	Moderado
		Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.	Uso no autorizado del equipo.	4	5	20	Sin control	1	20	Inaceptable	A.10.8.1 Políticas y procedimientos para el intercambio de información.	5	2	3	3	7	Moderado

Anexo A. (Continuación).

Número	Activos	Vulnerabilidad	Amenaza	Impacto	Probabilidad de ocurrencia	Riesgos (inherente)	Control existente	Eficacia control existente	Riego residual para control existente	Nivel de aceptación del riesgo	Controles sugeridos	Tiempo de implementación [días]	Costo de implementación	Valoración de incidencia	Costo- beneficio	Riesgo residual para controles sugeridos	Nivel de aceptación del riesgo
4	LUGAR	Red energética inestable	Pérdida del suministro de energía	4	5	20	Sin control	1	20	Inaceptable	A.9.2.2 Servicios de suministro	5	2	4	4	5	Moderado
5	ORGANIZACIÓN	Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos	4	4	16	Sin control	1	16	Inaceptable	A.10.10.2 Monitoreo del uso del sistema	10	1	3	5	3	Aceptable
		Falta de procedimientos de identificación y evaluación de riesgos	Abuso de los derechos	4	4	16	Sin control	1	16	Inaceptable	A.14.1.2 continuidad del negocio y evaluación de riesgos	2	2	4	3	5	Moderado
		Falta de procedimiento formal para la autorización de la información disponible al público	Divulgación	4	3	12	Sin control	1	12	Moderado	A.6.1.5 Acuerdos sobre confidencialidad	5	1	4	3	4	Aceptable

Anexo A. (Continuación).

Número	Activos	Vulnerabilidad	Amenaza	Impacto	Probabilidad de ocurrencia	Riesgos (inherente)	Control existente	Eficacia control existente	Riego residual para control existente	Nivel de aceptación del riesgo	Controles sugeridos	Tiempo de implementación [días]	Costo de implementación	Valoración de incidencia	Costo- beneficio	Riesgo residual para controles sugeridos	Nivel de aceptación del riesgo
5	ORGANIZACIÓN	Falta de planes de continuidad	Falla del equipo	4	5	20	Sin control	1	20	Inaceptable	A.14.1.3 Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	2	2	5	3	7	Moderado
		Falta de políticas sobre el uso del correo electrónico	Error en el uso	4	5	20	Sin control	1	20	Inaceptable	A.10.8.1 Políticas y procedimientos para el intercambio de información	2	2	3	2	10	Moderado
		Falta de procedimientos para el manejo de información clasificada	Error en el uso	4	5	20	Sin control	1	20	Inaceptable	A.7.2.2 Etiquetado y manejo de información	2	1	3	2	10	Moderado
		Falta de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso	4	4	16	Sin control	1	16	Inaceptable	A.6.1.3 Asignación de responsabilidades para la seguridad de la información.	2	2	4	3	5	Moderado

Anexo A. (Continuación).

Número	Activos	Vulnerabilidad	Amenaza	Impacto	Probabilidad de ocurrencia	Riesgos (inherente)	Control existente	Eficacia control existente	Riego residual para control existente	Nivel de aceptación del riesgo	Controles sugeridos	Tiempo de implementación [días]	Costo de implementación	Valoración de incidencia	Costo- beneficio	Riesgo residual para controles sugeridos	Nivel de aceptación del riesgo
5	ORGANIZACIÓN	Falta de política formal sobre la utilización de computadores	Hurto de equipo	4	2	8	Sin control	1	8	Moderado	A.5.1.1 Documento de la política de Seguridad de la información.	5	2	3	3	3	Aceptable

Anexo B. Encuesta jefe de infraestructura.

Encuesta de seguridad Informática, estado actual de la empresa V&G Tecnología y soluciones.

1. ¿La empresa cuenta con algún tipo de seguridad informática? Si su respuesta es Sí, menciónela.

- Si [X]
- No [ ]

Cual: Firewall con las respectivas reglas como son:

- VPN: Para controlar las conexiones.
- Web Filtering: Control a través de HTTP y HTTPSWeb, filtrado opciones de filtrado Web URL, palabra clave, tipo de archivo y base de datos.
- Control de aplicaciones: No.
- Ips: Detector de intrusos.
- Trafficshaping: controlar el ancho de banda.
- Dlp: Evitar fugas de información a través de USB.

- Antivirus: prevención de malware.

Anexo B. (Continuación).

- Antispam: Para prevenir correos basuras.
- Utm: gestión unificada de amenazas.
- Las actualizaciones de los antivirus se realizan de manera automática.

2. ¿La empresa cuenta con una política de seguridad?

- Si [X]
- No [ ]

Cual: Control de Ingreso de Personal por medio de un lector Biométrico.

3. ¿El acceso a internet es limitado?

- Si [ ]
- No [X]

4. ¿Qué tipo de herramientas de seguridad tiene implementado?

- Software [X]
- Hardware [X]

Anexo B. (Continuación).

5. ¿Cuáles son las tecnologías utiliza en la empresa?

- Virtualización [X]
- Backup [X]
- Disco Raid [X]

6. ¿Cuál de estos hardware de Seguridad es utilizado en la empresa?

- Llave USB O Hardkey [X]
- Lector [X]
- Otros [ ]

7. ¿Tiene instaladas sistemas de alimentación eléctrica?

- Si [ ]
- No [x]

Anexo B. (Continuación).

8. ¿Tiene personal especializado en seguridad informática?

- Si [ ]
- No [X]

9. ¿Cada cuánto la persona recibe cursos de actualizaciones con respecto a temas de seguridad informática?

- 1 mes a 2 meses [ ]
- 2 meses a 3 meses [ ]
- 3 meses a 6 meses [X]

10. ¿La empresa tiene plan contingencia?

- Si [ ]
- No [X]

Anexo B. (Continuación).

11. ¿La empresa tiene plan contingencia de continuidad de negocio?

- Si [ ]
- No [X]

12. ¿Qué debilidades tiene la empresa?

- No cuenta con un área de seguridad informática sólida.
- No se tiene una planta física en el caso de un riesgo eléctrico.
- No tener restringido el acceso a internet.
- No tener restringida el área del acceso a los servidores.
- No tener un registro de acceso para personas externas.

13. ¿Qué tan importante es la seguridad informática para la empresa?

Para la empresa es muy importante, pero no será implementado de una manera sólida ya que implica un costo bastante alto.

ANÁLISIS Y PLAN DE GESTIÓN DE RIESGOS PARA UNA EMPRESA OUTSOURCING DE DESARROLLO DE SOFTWARE PARA LA BANCA

Ávila Velandia Gineth
ginethav@gmail.com
Bobadilla Moreno Luis Carlos
luisbobadillamoreno@gmail.com
Universidad Piloto de Colombia
Especialización en Seguridad Informática, Cohorte XXIV
Bogotá, Colombia

RESUMEN: *Este artículo propone la implementación de un análisis de riesgo y plan de gestión de riesgos para los procesos del área de desarrollo de una empresa desarrolladora de software en donde se define parámetros como metodologías de seguridad de la información, aplicándolos a los requerimientos y necesidades de la empresa.*

PALABRAS CLAVE: Análisis de riesgo, vulnerabilidades, amenazas, impacto, controles, plan de gestión de riegos.

ABSTRACT: *This article proposes the implementation of a risk analysis and risk management plan for the area process of developing a software development company where parameters are defined as methods of information security, applying them to the requirements and needs of the company.*

I. INTRODUCCIÓN

Las organizaciones de hoy están expuestas frecuentemente a riesgos que pueden afectar directamente la misión, visión y sus objetivos. Los planes de gestión de riesgos facilitan a la organización los medios necesarios para identificar, analizar y tratar los riesgos que se puedan presentar, medir su magnitud y definir la forma de responder ante ellos, de manera que no se afecten los intereses, el patrimonio y la responsabilidad de la organización. De igual forma se generan los controles y así dar un óptimo tratamiento a los riesgos que se presenten, siendo un plan para la protección de los objetivos del negocio.

El propósito de la presente propuesta del plan de gestión de riesgos para el área de desarrollo de la organización es minimizar los riesgos, tomando como referencia la norma ISO/IEC 27005, la norma ISO/27001 y la norma técnica colombiana de Gestión del Riesgo NTC 5254.

II. LA EMPRESA

La empresa VYG Tecnologías y soluciones fue creada en el año 2007, desde entonces ha desarrollado proyectos principalmente para el sector financiero entre los que sobresalen la integración de servicios entre importantes entidades del país, para el año 2010 se inició en la prestación de servicios profesionales para lo cual se cuenta con efectivos procesos de selección, evaluación y contratación .

Es una empresa compuesta por 140 personas que se desempeñan en las áreas de gerencia, recursos humanos, infraestructura, desarrollo, calidad y gestión de proyectos.

A. PLANTEAMIENTO DEL PROBLEMA

¿De qué forma la empresa V&G Tecnología y Soluciones podrá manejar los riesgos operacionales en el área de desarrollo para no afectar el desempeño del área y la eficacia del servicio de la empresa?

B. OBJETIVO DEL PROYECTO

Realizar una propuesta de gestión de riesgo operativo en el área de desarrollo de VYG tecnología y soluciones, con el fin de proporcionarle una mayor seguridad a la información.

C. DISEÑO METODOLÓGICO

Este proyecto está orientado hacia una metodología de investigación de tipo descriptiva y explicativa, por lo tanto el desarrollo metodológico se ejecutara de acuerdo a los parámetros y directrices planteados en la norma NTC 5254, ISO/IEC 27001 y ISO/IEC 27005.

.

D. DISEÑO METODOLÓGICO

En este proyecto está orientado hacia una metodología de investigación de tipo descriptiva y explicativa por lo tanto el desarrollo metodológico se ejecutara de acuerdo a los parámetros y directrices planteados en la norma NTC 5254, ISO/IEC 27001 y la norma ISO/IEC 27005.

III. . FASES SEGÚN EL TEMA

A. Identificación y valoración de los activos

Se realiza la valoración de los activos con respecto a los tres elementos de la seguridad de la información, que son confidencialidad, integridad y disponibilidad. Para ello se investigó con cada uno de los responsables.

B. Identificación de las vulnerabilidades, amenazas y cálculo de los riesgos.

Después de haber identificado y valorado los activos se inicia el proceso de identificar las vulnerabilidades y amenazas, clasificándolas por cada tipo de activo según la norma ISO/IEC 27005 para el cálculo de los riesgos.

C. Planteamiento de acciones para gestión de riesgos

Terminadas las dos fases anteriores se procede a la identificación de los controles para los riesgos y las medidas de defensa teniendo en cuenta el impacto y el nivel de aceptación de los riesgos en la organización.

IV. DESARROLLO Y EJECUCIÓN DEL PROYECTO

El cálculo de los riesgos de seguridad de información incluye normalmente el análisis y la evaluación del riesgo. El análisis del riesgo domina:

- ✓ Identificación de los activos de información y valoración de impacto.
- ✓ Identificación de amenazas y vulnerabilidades para cada activo identificado.
- ✓ Cálculo de la probabilidad que las amenazas se materialicen a través de una vulnerabilidad.

La evaluación del riesgo incluye:

- ✓ Cálculo del riesgo.
- ✓ Controles Existentes
- ✓ Calculo del riesgo residual
- ✓ Identificación del riesgo inherente a la Matriz de Niveles de riesgo.

V. . ANÁLISIS DE RIESGO

A. Identificación de Activos

De acuerdo con el diseño metodológico, en la primera fase se realiza la identificación de los activos para el área de desarrollo, por medio de encuestas con el ingeniero de infraestructura y responsable del área las cuales se anexan en el presente trabajo

Se efectuó la clasificación de los activos de acuerdo a la norma ISO/IEC 27005 en su anexo B, como se enseña en el cuadro 1 y se realizó la valoración de cada activo de acuerdo a los principios de seguridad de la información que es: la confidencialidad, la integridad y disponibilidad.

CUADRO I
Ejemplo de valoración de Impacto de los activos

No	Tipos de activo	Activos	Integridad	Disponibilidad	Confidencialidad	Impacto
1	Hardware	Computadores de escritorio, Servidor, Disco Duro extraíble	4	4	4	4
2	Software	Sistemas Operativos y las aplicaciones del negocio	4	4	4	4
3	Personal	Usuarios finales, alta gerencia, líder de proyectos y desarrolladores	4	4	4	4
4	Lugar	Casa, oficinas y centro de cómputo.	4	4	4	4
5	Organización	servicio , proveedores, proyectos	4	4	4	4

Para la valoración dada en el cuadro 1, se estableció el valor cuatro (4) impacto mayor, que hace referencia a lesiones grandes, pérdida de la capacidad de producción y pérdida financiera importante.

B. Identificación de las amenazas

Se Inicia el proceso de evaluación de las amenazas con respecto a la norma ISO/IEC 27005 en su anexo C. Estas pueden explotar una o varias vulnerabilidades; al no tener un control sobre las amenazas estas pueden presentar incidentes que afectan a la organización.

C. Identificación de vulnerabilidades

Terminado el proceso de identificar las amenazas y los activos evidenciamos con ayuda de la norma ISO/IEC 27005 en su anexo D, que las amenazas identificadas explotan 21 vulnerabilidades.

D. Probabilidad de ocurrencia

Una vez identificadas las amenazas y vulnerabilidades se evalúa la probabilidad que una amenaza llegue a explotar una vulnerabilidad y causar un riesgo, se tomó como referencia la norma NTC 5254 en su anexo E.

V. EVALUACIÓN DEL RIESGO

A. Cálculo del riesgo

Al obtener las amenazas, vulnerabilidades y los diferentes valores enunciados en los cuadros se obtuvo como resultado el análisis de riesgos, de acuerdo a esto se obtiene el riesgo inherente con la siguiente ecuación: Riesgo inherente= impacto * probabilidad de ocurrencia

B. Nivel de aceptación de riesgo

Para el cálculo de nivel de aceptación de riesgo se toma como referencia la norma ISO/IEC 27005 en su anexo E. En conjunto con la gerencia y los encargados de los procesos del área de desarrollo, de acuerdo a las consecuencias evaluadas y la probabilidad.

CUADRO II.
Nivel de aceptación y valor del riesgo

Nivel de aceptación	Valor
Aceptable	1-4
Moderado	5-14
Inaceptable	15-25

C. Controles Existentes

Como se sugiere en la norma ISO/IEC 27005 numeral 8.2.1.4 se identifican los controles existentes para evitar trabajo y costos innecesarios, por ejemplo duplicación de los controles.

D. Cálculo del riesgo residual

El excedente del riesgo inherente al aplicar sobre un control, es llamado riesgo residual y se calcula mediante la siguiente formula: Riego residual = riesgo inherente / valoración del control.

VI. PLAN DE GESTIÓN DE RIESGOS

El plan de gestión de riesgos se realiza aplicando controles sugeridos con el objetivo de minimizar los riesgos que se evidencian en el proceso de evaluación de riesgos, los que están en un nivel inaceptable y moderado.

A. Cálculo del valor Costo – Beneficio

Se deberán asignar tres valores para la valoración de cada control: el primero de acuerdo al costo de implementación, el segundo de acuerdo al tiempo de implementación y por último, la valoración del incidente en el caso de que no se implemente dicho control. Para evaluar objetivamente cada uno de estos parámetros se han definido las métricas que se presentan a continuación:

CUADRO III
Costo de implementación

Valor cuantitativo	Valor cualitativo	Detalle
1	Menor	Menor a un SMMLV
2	Bajo	De 1 a 5 SMMLV
3	Medio	De 5 a 10 SMMLV
4	Alto	De 15 a 20 SMMLV
5	Muy Alto	Mayor a 20 SMMLV

CUADRO IV
Tiempo de implementación

Valor cuantitativo	Valor cualitativo	Descripción
1	Menor	1 a 3 días
2	Bajo	Inferior a 4semanas
3	Medio	Inferior a 10 semanas
4	Alto	Inferior a 15 semanas
5	Muy alto	Superior a 20 semanas

CUADRO V
Valoración de un incidente si no se implementa el control

Valor	Impacto	Descripción
1	Insignificante	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas insignificantes.
2	Bajo	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas bajas.
3	Moderado	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas moderadas.
4	Alto	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas altas.
5	Extremo	La pérdida de confidencialidad, Integridad o Disponibilidad generará pérdidas totales.

Después de realizar la valoración respectiva de los tres criterios mencionados anteriormente, estas valoraciones serán tomadas para obtener un promedio de la siguiente forma, Costo-beneficio = ((costo de implementación +tiempo de implementación +valoración de incidente) / 3).

Posteriormente de obtener el valor definido del costo-beneficio, este será evaluado frente a la métrica que se presenta a continuación el en cuadro VI:

CUADRO VI
Valoración Costo-Beneficio

Valor	Descripción
1	No se implementa el control
2	El costo – Beneficio tiene un valor bajo
3	El costo – Beneficio tiene un valor medio
4	El costo – Beneficio tiene un valor alto
5	El costo – Beneficio tiene un valor muy alto

VII. ANÁLISIS DE RESULTADO

El análisis de resultado consiste en evaluar los resultados de la matriz y tomar estos para generar estadísticas frente al análisis de riesgos y el plan de gestión de riesgos.

Para el análisis de resultados, se individualizó los aspectos más importantes, distribuidos de la siguiente forma:

A. Vulnerabilidad con mayor número de incidencias

De las 21 vulnerabilidades identificadas, a continuación en la figura 1 se enuncian las 10 con mayor número de incidencias en la empresa:

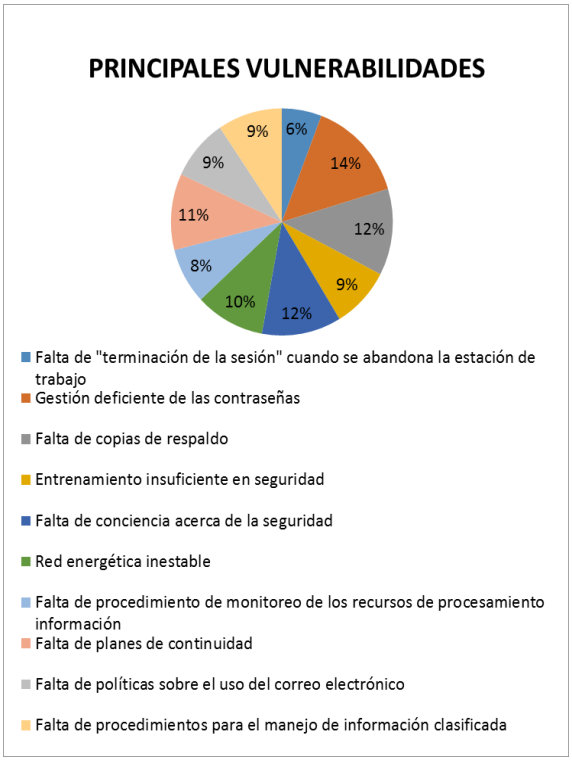


Fig. 1Principales Vulnerabilidades

B. Amenazas con mayor número de incidencias

De las 14 amenazas detectadas, a continuación se muestran en la figura 2 las 10 principales que afectan los procesos del área de desarrollo de la organización, al igual que el número de incidencias presentadas por cada amenaza.

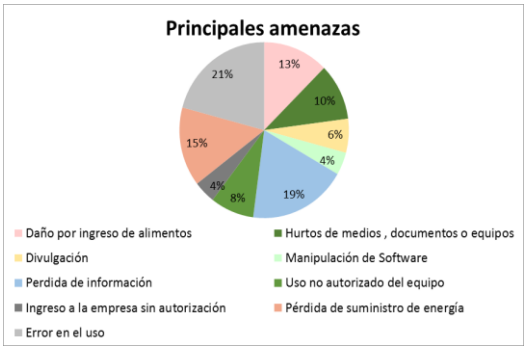


Fig. 2 Principales Amenazas

C. Valoracion de riesgo

En la figura 3 se visualiza el porcentaje de riesgos antes de la implementación de los controles sugeridos

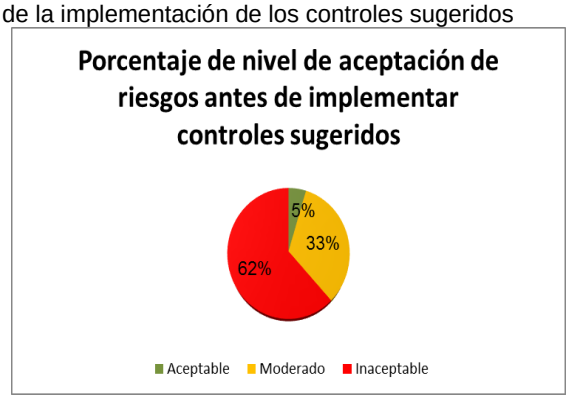


Fig. 3 Porcentaje de nivel de aceptaciòn de risgos antes de implementar controles sugridos

Como se aprecia en la Figura 3, más de la mitad de los riesgos hallados (62%) en los procesos en estudio se encuentra en la zona inaceptable de acuerdo a la valoración realizada para el presente proyecto y el (38%) restante están en la zona aceptable y moderada, se determinó evaluar y tratar todos los riesgos ya que actualmente la empresa tiene bajo nivel de seguridad en el área de desarrollo y tiene implementados pocos controles, y la mayoría son ineficientes.

D. Controles màs sugeridos

De acuerdo a la norma ISO/IEC 27001 en su anexo A, se precisaron 16 controles para 21 vulnerabilidades y 14 amenazas. Los controles con mayor número de riesgos fueron:

- ✓ A.8.2.2 Educación, formación y concientización sobre la seguridad de la información.
- ✓ A.9.2.2 Servicios de suministro.
- ✓ A10.8.1 políticas y procedimientos de intercambio de información
- ✓ A.10.10.2 Monitoreo del uso del sistema.
- ✓ A.11.5.2 identificación y autenticación de usuarios

E. Costo – Beneficio

La evaluación para cada uno de los controles que fueron sugeridos desde el punto de vista costo beneficio se valora en función del costo implementación del control sugerido, el tiempo de implementación y la pérdida de imagen de la empresa omisión en su implementación

De acuerdo con los valores de Costo – Beneficio, se asignan a 5 como valor muy alto, a 4 valor alto, a 3 valor medio y a 2 Valor bajo.

Los controles a implementar generan un beneficio alto a bajo-costo, por lo tanto, se recomienda implementar estos controles.

F. Resultado obtenido del plan de gestión de riesgos

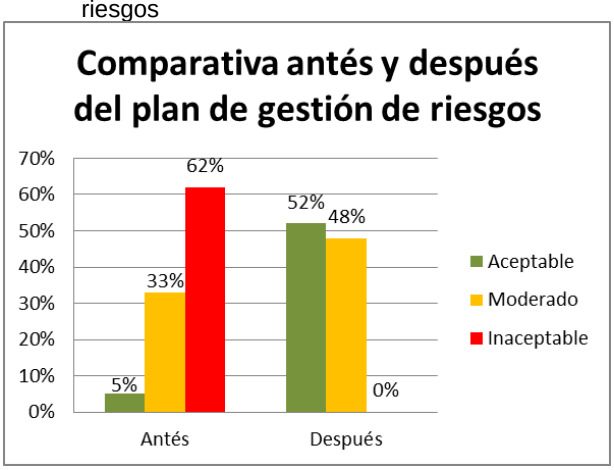


Fig. 4 Comparativa antes y después del plan de gestión de riesgos

Como se observa en la figura 4 en lo que respecta a la mitigación del riesgo de un total de (62%) riesgos en el rango inaceptable pasaron a (0%), de (33%) en nivel moderado pasaron a (48%) y de un total de (5%) riesgos en nivel aceptable, pasaron a (52%).

VIII. CONCLUSIONES

Al hallar los riesgos residuales se concluyó que los controles existentes en la organización son insuficientes.

Al realizar el análisis del riesgo se detectaron 14 amenazas y 21 vulnerabilidades.

Se encontraron 205 activos para el área de desarrollo.

Las principales vulnerabilidades que presentan los activos son: gestión deficiente de las contraseñas (14%), falta de copias de respaldo (12%) y falta de conciencia acerca de la seguridad (12%).

El 5% de los riesgos se encuentran en el rango aceptable, el 33% en el rango moderado y el 62% de los riesgos se presentan como inaceptables.

En cuanto a controles, de acuerdo con la norma ISO/IEC 27001 en su anexo A, se precisaron 16 controles para 21 vulnerabilidades y 14 amenazas.

Los controles que aplican para un mayor número de riesgos son A.8.2.2 Educación, formación y concientización sobre la seguridad de la información (10%), A.9.2.2 Servicios de suministros, (10%), A10.8.1 políticas y procedimientos de intercambio de información (10%), A.10.8.1 Monitoreo del uso del sistema (10%), A.11.5.2 identificación y autenticación de usuarios (10%). Los controles anteriormente mencionados están de acuerdo a la norma ISO/IEC 27001:2005 en su anexo A.

En lo que respecta a la mitigación del riesgo de un total de (62%) de riesgos en el rango inaceptable pasaron a (0%), de (33%) en nivel moderado pasaron a (48%) y de un total de (5%) riesgos en nivel aceptable, pasaron a (52%) después de los controles sugeridos.

Después de realizar el análisis de riesgo, y teniendo en cuenta que los controles aplican para mitigar los riesgos están en el rango inaceptable, moderado, se elaboró el plan de gestión de riesgos, cuyos datos obtenidos están inmersos en la matriz de resultados. Se recomienda a la organización seguir el plan de gestión de riesgos propuesto.

BIBLIOGRAFIA

[1] INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Norma Técnica Colombiana para la Tecnología de la información, técnicas de seguridad de la información (SGSI), requisitos. Bogotá D.C, ICONTEC, 2006.NTC-ISO/IEC 27001.

[2] INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Norma Técnica Colombiana para la Gestión de riesgo. Bogotá D.C, ICONTEC, 2008.NTC- 5254.

[3] INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Norma Técnica Colombiana para la presentación de tesis, trabajos de grado y otros trabajos de investigación. Bogotá D.C, ICONTEC, 2008. NTC 1486.

[4] INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Norma Técnica Colombiana para referencias documentales para fuentes de información electrónicas. Bogotá D.C, ICONTEC, 2008. NTC 4490.

[5] INSTITUTO COLOMBIANO DE NORMAS TÈCNICAS. Norma Técnica Colombiana para la presentación de tesis, trabajos de grado y otros trabajos de investigación. Bogotá D.C, ICONTEC, 2008. NTC 1486.